Навчально-методичне видання

**О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук,
Ю.М. Ткач, Є.В. Іванченко**

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

В авторській редакції

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 05.06.2019 р.
Формат 60х 84/16. Папір офсетний. Друк числовий.
Гарнітура Times New Roman. Обл.-вид. арк. 23,40.
Ум. друк. арк. 23,72. Тираж 300 прим.
Зам. № 571.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

*Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ДК № 3020 від 02.11.2007 р.*

*16600, Чернігівська обл., м. Ніжин, вул. Небесної сотні, 13 а.
Тел.: 068 815 06 60
E-mail: holdingvv@ gmail.com*

**О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук,
Ю.М. Ткач, Є.В. Іванченко**

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Чернігів
2019

УДК 004.056.5
М 50

Рецензенти:

д.т.н., проф. Є.В. Василіу,
д.т.н., проф. О.А. Смірнов,
д.т.н., проф. Ю.Є. Яремчук.

Рекомендовано до друку Вченою радою Чернігівського національного технологічного університету (протокол № 3 від 25.03.2019 р.)

М-50 Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.

ISBN 978-617-7609-35-2

У навчальному посібнику розкрито питання менеджменту інформаційної безпеки, а саме, сутність та завдання менеджменту інформаційної безпеки, складові системи менеджменту інформаційної безпеки, процеси ризик-менеджменту, засоби реалізації й підтримки функціонування системи менеджменту інформаційної безпеки та її аудит. Виклад теоретичного матеріалу доповнено практичними завданнями, кожен розділ завершено питаннями для самоконтролю.

Посібник призначено для студентів спеціальності 125 «Кібербезпека» першого освітнього рівня підготовки (бакалавр), а також буде корисним магістрам (другий освітній рівень) відповідної спеціальності, аспірантам, викладачам, науковцям та фахівцям у галузі інформаційної безпеки.

УДК 004.056.5

ISBN 978-617-7609-35-2

СПИСОК ЛІТЕРАТУРИ ДО П'ЯТОГО РОЗДІЛУ

1) «Настанови щодо здійснення аудитів систем управління», ДСТУ ISO 19011:2012, Національний стандарт України, 2012, с. 34.

2) «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

3) А.А. Дмитриев: «Внутренний аудит системы менеджмента информационной безопасности по требованиям ISO/IEC 27001. один из вариантов реализации процесса», «Das Management» №2, 2011, с. 58-64.

4) «Про аудит фінансової звітності та аудиторську діяльність», Закон України, ВР від 21.12.2017р. № 2258-VIII. [Електронний ресурс], Режим доступу: http://search.ligazakon.ua/ l_doc2.nsf/ link1/T172258.html (26 січня 2019).

Питання для самоконтролю

1) Що таке аудит ІБ?
2) Який стандарт регламентує проведення внутрішніх аудитів?
3) Які етапи внутрішнього аудиту СМІБ?
4) Які існують принципи проведення внутрішнього аудиту СМІБ?
5) Що таке сертифікований аудит СМІБ?

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ……. 5
ВСТУП…….. 7
Розділ 1. СУТНІСТЬ ТА ЗАВДАННЯ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ…… 9
1.1. Базові поняття менеджменту…… 9
1.2. Базові характеристики інформаційної безпеки 24
1.3. Базові поняття системи менеджменту інформаційної безпеки……..…… 29
1.4. Місце і види інформації……...…… 32
1.5. Цикл PDCA……..……. 35
1.6. Діяльність міжнародних організацій у сфері інформаційної безпеки…… 39
1.7. Діяльність спеціалізованих міжнародних організацій і об'єднань в сфері інформаційної безпеки……. 50
1.8. Серія стандартів ISO / IEC 27000. Історія стандарту ISO / IEC 27001…… 58
СПИСОК ЛІТЕРАТУРИ ДО ПЕРШОГО РОЗДІЛУ…… 69
Розділ 2. СКЛАДОВІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СМІБ)…….. 71
2.1. Переваги впровадження СМІБ…… 71
2.2. Сфери дії СМІБ……...….. 74
2.3. Інтеграція СМІБ та системи менеджменту якості……. 77
2.4. Відповідальність керівництва…… 78
2.5. Цілі інформаційної безпеки та планування їх досягнення..... 83
2.6. Забезпечення СМІБ…….. 110
2.7. Функціонування СМІБ…… 116
2.8. Оцінка ефективності СМІБ…… 121
2.9. Вдосконалення СМІБ…….. 125
СПИСОК ЛІТЕРАТУРИ ДО ДРУГОГО РОЗДІЛУ…….. 127
Розділ 3. ПРОЦЕСИ РИЗИК-МЕНЕДЖМЕНТУ…… 128
3.1. Міжнародні стандарти оцінювання інформаційних ризиків…….. 129
3.2. Сучасні методи і засоби оцінювання ризиків… 141

3.3. Сучасні бази даних уразливостей інформаційної безпеки…… 180
3.4. Оцінювання ризиків інформаційної безпеки… 212
3.5. Обробка ризиків інформаційної безпеки…….. 226
3.6. Прийняття ризику інформаційної безпеки…… 231
СПИСОК ЛІТЕРАТУРИ ДО ТРЕТЬОГО РОЗДІЛУ…… 233
Розділ 4. ЗАСОБИ РЕАЛІЗАЦІЇ ТА ПІДТРИМКИ ФУНКЦІОНУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ…… 240
4.1. Політики інформаційної безпеки…… 240
4.2. Організаційне забезпечення інформаційної безпеки…….. 247
4.3. Безпека персоналу…… 254
4.4. Управління активами……... 263
4.5. Управління доступом…… 295
4.6. Криптографічне забезпечення…… 308
4.7. Системи фізичної безпеки……... 312
4.8. Безпека виробничих процесів…… 324
4.9. Безпека комунікацій…… 338
4.10. Впровадження та експлуатація інформаційних систем…… 345
4.11. Відносини з постачальниками…….. 357
4.12. Управління інцидентами інформаційної безпеки…… 364
4.13. Забезпечення безперервності бізнесу…….. 370
4.14. Відповідність нормативно-правовому забезпеченню…….. 373
СПИСОК ЛІТЕРАТУРИ ДО ЧЕТВЕРТОГО РОЗДІЛУ….. 381
Розділ 5. АУДИТ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……..... 383
5.1. Внутрішній аудит…… 383
5.2. Зовнішній аудит…… 400
СПИСОК ЛІТЕРАТУРИ ДО П'ЯТОГО РОЗДІЛУ…….. 407

Складовою частиною звіту про результати аудиту можуть бути заповнені опитувальні листи, переліки контрольних питань, результати спостереження, журнали реєстрації або зауваження аудитора.

У випадку використання відповідних методів ці документи мають подаватися до органу сертифікації як свідчення для підтримки рішення про сертифікацію. Інформацію по вибірках, оцінених під час аудиту, слід включити в звіт про результати аудиту або в іншу документацію по сертифікації.

У звіті повинна розглядатися правильність внутрішньої структури і процедур, прийнятих організацією-клієнтом для забезпечення довіри до СМІБ. На додаток до вимог, що пред'являються до складання звітів ISO/IEC 17021.

Звіт повинен містити:

– ступінь довіри до внутрішніх аудитів СМІБ і перевіркам з боку керівництва;

– короткий виклад найбільш важливих спостережень як позитивного, так і негативного характеру, що стосуються впровадження та результативності СМІБ;

– рекомендацію аудиторської групи щодо того, чи слід сертифікувати СМІБ організації-клієнта з інформацією для обґрунтування цієї рекомендації.

Проведення перевірки системи менеджменту є надзвичайно необхідним процесом, адже вона дозволяє дослідити стан СМІБ. Виявити недоліки, які необхідно врахувати і виправити для позитивного функціонування, але підходити до проведення перевірки потрібно дуже ретельно. Необхідно підбирати кваліфікованих аудиторів, перевіряти їх рівень знань. Обирати оптимальні етапи для проведення перевірки та надання всіх необхідних умов для якісної сертифікації об'єкта. Уважно слідкувати за веденням документації. А також робити висновки та реалізовувати їх у СМІБ.

Проведення аудиту також є обов'язковим згідно законодавства України.

ності та продуктивності аудиту, а також підтримання цілісності процесу аудиту.

6) Оцінка аудиту, звітність (ведення записів, невідповідності). Орган сертифікації може використовувати різні процедури, пов'язані з складанням звітів, що відповідають його потребам, але ці процедури, як мінімум, повинні забезпечити наступне: до того, як аудиторська група покине територію організації-клієнта, проводиться зустріч аудиторської групи та керівництва організації-клієнта, в ході якої аудиторська група:

– в письмовій або усній формі повідомляє про відповідність СМІБ організації-клієнта визначеним вимогам сертифікації;

– надає можливість представникам організації-клієнта задавати питання про зроблені висновки і про підстави для них;

– подає до органу сертифікації звіт про результати аудиту щодо відповідності СМІБ організації-клієнта всім вимогам сертифікації.

У звіті про результати аудиту повинна бути представлена наступна інформація:

– короткий аналіз документів;

– аналіз ступеня ризику ІБ організації-клієнта;

– загальний час, витрачений на аудит, і докладний опис часу, витраченого на аналіз документів, оцінку аналізу ризиків, аудит на місцях та складання звітів про результати аудиту: питання аудиту, основна причина їхнього вибору і застосована методологія.

Звіт про результати аудиту, представлений органу сертифікації, повинен бути достатньо докладним для спрощення прийняття рішення про сертифікацію та його підтримку і повинен містити:

– області, включені в аудит (наприклад, вимоги сертифікації та перевірені об'єкти), включаючи значущі контрольні записи і використані методи аудиту;

– спостереження як позитивного (наприклад, що заслуговують уваги особливості), так і негативного (наприклад, потенційні невідповідності) характеру;

– подробиці виявлених невідповідностей, підтверджені об'єктивними даними, і посилання цих невідповідностей на відповідні вимоги стандарту ISO / IEC 27001 зі СМІБ або інші документи, необхідні для сертифікації.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІС	-	Автоматизована інформаційна система;
АОР	-	Аналіз та оцінювання ризиків;
БД	-	База даних;
ЕІ	-	Електронна інформація;
ЗЗІ	-	Засоби захисту інформації;
ЗІ	-	Захист інформації;
ІА	-	Інформаційний актив;
ІБ	-	Інформаційна безпека;
ІС	-	Інформаційна система;
ІТ	-	Інформаційні технології;
КЛ	-	Кількісні;
МБМ	-	Метод на основі байєсовских мереж;
МР	-	Міра ризику;
НАС	-	Неавторизована сторона;
НСД	-	Несанкціонований доступ;
НСМ	-	Несанкціонована модифікація;
НТР	-	Науково-технічна революція;
ОЗ	-	Оцінювання загрози;
ОР	-	Оцінювання ризиків;
ОС	-	Операційна система;
ПБ	-	Політика безпеки;
ПЗ	-	Програмне забезпечення;
ПК	-	Персональний комп’ютер;
РІС	-	Ресурси інформаційних систем;
РП	-	Ризикоутворюючий потенціал;
РР	-	Рівень ризику;
СЗІ	-	Система захисту інформації;
СМІБ	-	Система менеджменту інформаційної безпеки;
СМР	-	Ступінь можливості реалізації;
СМЯ	-	Система менеджменту якості;
СТН	-	Ступінь тяжкості наслідків;
ТО	-	Тематичний опитувальник;
ЦО	-	Цільові об'єкти;
ЯК	-	Якісні;
EFMD	-	European Foundation for Management Development;

IEC	-	International Electrotechnical Commission;
ISO	-	International Organization for Standardization;
PDCA	-	Plan-Do-Check-Act.

значати область дії сертифікації та складу стандарту ISO/IEC 27001 з СМІБ, за яким ця СМІБ сертифікована. Крім того, в сертифікаті має бути посилання на певну версію Положення про застосування. Список сертифікованих клієнтів.

Застосовуються вимоги ISO/IEC 17021. Посилання на сертифікацію та використання маркування. Крім того, застосовуються ще деякі специфічні для СМІБ вимоги і положення.

Доступ до документів організації. Перед проведенням аудиту орган сертифікації повинен зробити запит організації-клієнта про наявність документів про СМІБ, які не можуть бути надані для перевірки аудиторської групи, так як вони містять конфіденційну або секретну інформацію. Орган сертифікації повинен визначити чи може бути адекватним проведення аудиту СМІБ при відсутності цих документів. Якщо орган сертифікації приходить до висновку, що неможливо провести аудит СМІБ адекватно без перевірки конфіденційних або секретних документів, він повинен попередити організацію-клієнта, що сертифікаційний аудит не може бути проведений до тих пір, доки не буде забезпечений доступ до цих документів. Обмін інформацією між органом сертифікації і його клієнтами застосовуються вимоги ISO / IEC 17021.

5) Методика аудиту. Орган сертифікації повинен передбачати процедури, що дозволяють вимагати від організації-клієнта можливість продемонструвати, що внутрішні аудити СМІБ сплановані, а програма і процедури їх проведення стають чинними. Процедури органу сертифікації не повинні припускати особливого способу реалізації СМІБ або особливого формату для документації і записів. Процедури сертифікації повинні концентруватися на встановленні того, що СМІБ організації-клієнта відповідатиме вимогам стандарту ISO/ IEC 27001, а також політиці і цілям організації-клієнта.

План аудиту має визначати методи аудиту із застосуванням мережевих технологій, які будуть при необхідності під час аудиту. *Примітка*. Методи аудиту із застосуванням мережевих технологій можуть включати, наприклад, телеконференції, Інтернет-наради, інтерактивний зв'язок на базі Інтернет-технологій та віддалений електронний доступ до документації СМІБ та / або процесам СМІБ. Метою застосування таких методів має бути підвищення ефектив-

якої вони діють. Компетентність аудиторів може бути встановлена на основі підтвердженого досвіду чи спеціального навчання або шляхом співбесіди.

2) Підготовка аудитора. Підготовка аудитора полягає у його обізнаності в сфері проведення сертифікації. Для якісної оцінки аудитор повинен бути перевірений на:

– знання стандарту СМІБ та інших відповідних нормативних документів;
– розуміння питань ІБ;
– розуміння оцінки ризику та менеджменту ризику з точки зору діяльності;
– технічні знання про діяльність, що підлягає аудиту;
– знання систем менеджменту;
– загальне знання нормативних вимог щодо СМІБ;
– розуміння принципів аудиту, заснованих на ISO 19011;
– знання аналізу ефективності СМІБ та вимірювання ефективності засобів контролю.

При необхідності аудиторська група може доповнятись технічними експертами, які повинні володіти спеціальними знаннями в області технології, що підлягає аудиту. Необхідно зазначити, що технічних експертів не можна використовувати замість аудиторів СМІБ, але вони можуть консультувати аудиторів з питань технічної адекватності в контексті системи менеджменту, яка піддається аудиту.

3) Вступна нарада. На вступній нараді оголошуються етапи робіт, які проводитиме аудитор, а саме:

– обстеження об’єкту сертифікації;
– аналіз інформаційних ризиків;
– обробка даних та підготовка рекомендацій;
– складення та надання звіту про аудит.

Встановлюються області проведення аудиту, інформація до якої аудитор має право доступу, термін проведення сертифікації.

4) Документи на аудит. Орган сертифікації повинен надати кожній зі своїх організацій-клієнтів, чия СМІБ сертифікується, документи з сертифікації, як лист або сертифікат, підписаний уповноваженою посадовою особою. Для організації-клієнта і кожної з її сертифікованих інформаційних систем ці документи повинні ви-

ВСТУП

Сьогодні в умовах активного розвитку та впровадження сучасних інформаційних технологій (ІТ) та засобів обчислювальної техніки, інфраструктура підприємств та держаних установ набуває неструктурованого характеру, що тягне за собою неконтрольоване зростання уразливостей та загроз інформаційній безпеці (ІБ) організації та держави в цілому. З часом кількість загроз та інтенсивність їх реалізації може набути неконтрольованого характеру, а отже значна частина організацій (різних джерел фінансування) залишається незахищеною перед сучасними викликами інформаційного простору. Таким чином, виникає необхідність у забезпеченні ІБ як державних так і недержавних установ, тобто з’являється потреба у впроваджені системи менеджменту інформаційної безпеки (СМІБ).

У сімействі міжнародних стандартів СМІБ (ISO/IEC 27000) ІБ (*information security*) тлумачиться як збереження конфіденційності (*confidentiality* – властивість, яка вказує, що інформація залишається недоступною або нерозкритою для неавторизованої сторони), цілісності (*integrity* – властивість збереження повноти і точності) і можливості застосування інформації. (*availability* – властивість доступності і готовності до використання за авторизованим запитом). Зауважимо, що система менеджменту (*management system*) являє собою сукупність взаємопов'язаних або взаємодіючих елементів організації для розробки політик і цілей, а також процесів для їх досягнення. Разом з тим, система менеджменту може бути спрямована на один або кілька об'єктів управління, при цьому до елементів системи менеджменту відносяться структура організації, ролі і відповідальності, планування, функціонування тощо.

Оскільки основою СМІБ є управління інформаційними ризиками та управління доступом (розмежування доступу), то саме ці аспекти впровадження СМІБ на основі використання чинних міжнародних стандартів є основною метою даного навчального посібника, який складається з таких складових: *перший розділ* висвітлює основні поняття менеджменту та менеджменту інформаційної безпеки, описує особливості серії міжнародних стандартів ISO/IEC 27000, розкриває історію створення стандарту ISO/IEC 27001 та суть діяльності міжнародних організацій в сфері інформаційної

безпеки; *другий розділ* присвячений сфері дії та перевагам впровадження СМІБ, у ньому визначається відповідальність керівника, оцінюється ефективність СМІБ та висвітлюються інших складові системи менеджменту інформаційної безпеки; *третій розділ* містить опис процесів ризик-менеджменту, а саме оцінювання, обробка та прийняття ризиків інформаційної безпеки; *четвертий розділ* розкриває особливості змістового наповнення та впровадження міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002, зокрема, криптографічне забезпечення, систему фізичної безпеки та безпеки виробничих процесів й комунікацій тощо; *п'ятий розділ* описує внутрішній та зовнішній аудит.

Навчальний матеріал, що міститься у навчальному посібнику, викладений логічно, у простій та доступній для розуміння формі. Теоретичний матеріал супроводжується практичними ситуаціями, що сприятиме більш ефективному засвоєнню висвітленої інформації. До кожного розділу пропонуються питання для самоконтролю, що охоплюють його основні теоретичні положення, а також список літератури.

Структура та зміст навчального посібнику визначені відповідно до робочої програми дисципліни «Менеджмент інформаційної безпеки» та з урахуванням Стандарту вищої освіти України галузь знань 12, спеціальність 125 «Кібербезпека».

Рис. 5.12. Алгоритм аудиту третьою стороною

1) Проведення аудиту та надання інших аудиторських послуг здійснюється аудиторами, аудиторськими фірмами, які набули права на здійснення аудиторської діяльності відповідно до Закону України «Про аудит фінансової звітності та аудиторську діяльність» [4].

Аудитором може бути фізична особа, яка має сертифікат, що визначає її кваліфікаційну придатність на заняття аудиторською діяльністю на території України.

Згідно міжнародного стандарту ISO/IEC 27006 – керівництво органу сертифікації повинно провести необхідні процедури та ресурси для визначення компетентності окремих аудиторів щодо завдань, які вони повинні виконати в області сертифікації, в рамках

Рекомендації. «Надійність і довіра до процесу аудиту залежать від кваліфікації тих фахівців, які здійснюють аудит!» (DIN EN ISO 19011 7.1 Загальні положення)

Висновок: Стати хорошим аудитором непросто, але витрачені зусилля компенсуються як Вам, так і Вашому підприємству! [3].

5.2. Зовнішній аудит

Аудит постачальника (аудит другою стороною) (перед контрактне обстеження) (див. рис. 5.11).

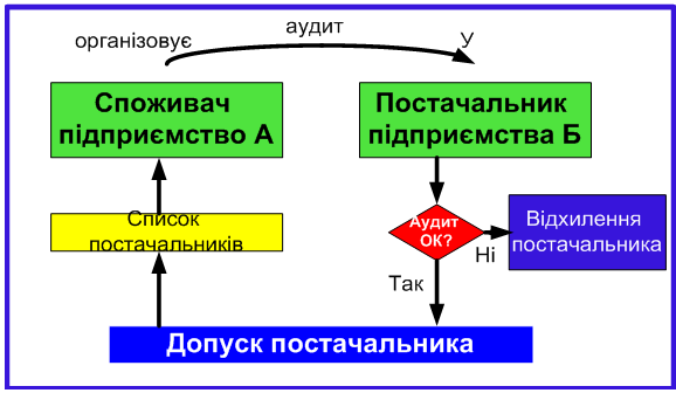


Рис. 5.11. Алгоритм аудиту зі сторони постачальника

Аудит замовника аудиту (аудит третьою стороною) (сертифікація, незалежна перевірка) (див. рис. 5.12).

Розділ 1. СУТНІСТЬ ТА ЗАВДАННЯ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Базові поняття менеджменту

Поняття менеджменту

Менеджмент у максимально широкому розумінні – це керівництво соціально-економічними системами. **Менеджмент** (керівництво) складається із двох функцій: організації та управління. Взаємозв'язок цих функцій визначається тим, що не можна управляти неорганізованою системою, тобто, чим краще організоване підприємство, тим менше воно має потребу в управлінні. Однак звести керівництво тільки до вдосконалювання організації роботи з метою ліквідації проблем управління неможливо через мінливі умови зовнішнього середовища.

Організація (як діяльність) – це утворення і удосконалення зав'язків між частинами цілого; створення та удосконалення структури і правил функціонування її елементів.

Управління – це процес (діяльність), спрямований на досягнення мети; перехід системи з одного стану в заданий або утримання в заданому. Управління соціально-економічними системами, у тому числі виробничими, одержало назву менеджмент (англ. management, від старофранцузького слова ménagement «мистецтво супроводжувати, направляти», від лат. manu agere «вказувати рукою» порівн. рос. керувати).

Менеджмент (від англ. manage – управляти, керувати) наука про організації діяльності соціальної системи для досягнення заданих цілей, в умовах обмеженості ресурсів (від лат. manus agere, manibus agere – робити руками), за змістом близько до російського слова «керувати» [1, 2]. Менеджер оперує об'єктами, речами та ситуаціями, для досягнення поставлених цілей і завдань. Також останнім часом менеджерами називають абсолютно будь-яку офісну одиницю, нехай навіть така одиниця виконує обслуговуючі функції. У багатьох автосалонах і магазинах менеджерами називають звичайних продавців, тим самим принижуючи значення цієї професії. Так, наприклад, у Південній Кореї і Японії, співробітник повинен проробити в компанії 10 – 15 років на найрізноманітніших, часто не високих посадах, що б дослужитися до посади менеджера.

Таким чином, можна констатувати, що в нашій країні слово «менеджер» застосовується зовсім не доречно, і носить характер кітчу. Так, у Радянському Союзі посаді «менеджер» відповідало цілком адекватне слово «начальник». **В українських умовах поняття «менеджмент» і «підприємництво»** стали широко вживатися наприкінці 80-х – початку 90-х рр. у зв'язку з перебудовою, що почалася у Радянському Союзі. Перехід від адміністративно-командної системи управління до ринкової зажадав змін, як у соціально-політичному житті суспільства, так і у всій економічній сфері. Необхідно було переглянути сформовану раніше систему управління, в основі якої лежали принципи централізованого директивного планування, твердого розподілу матеріальних, людських і фінансових резервів та ресурсів із центру. Потрібно було міняти всю систему підпорядкування та контролю, фундаментом якої були демократичний централізм, народний контроль і т. ін. Ринкові відносини припускають інший підхід до управління: більш демократичних методів роботи; нових взаємин «керівник – підлеглий»; наслідування твердим правилам ринку, конкуренції, приватного інтересу, а також прагнення людей отримати найбільшу вигоду від зробленої справи. Більші можливості для розвитку підприємництва відкрилися в результаті приватизації, що дозволила створити приватні підприємства, акціонерні товариства, асоціації і союзи в промисловості та інших галузях народного господарства. Нові економічні відносини зажадали не тільки підприємців, але і професійних керівників – менеджерів.

В наш час поняття «менеджер», «бізнесмен», «підприємець» широко використовується як у повсякденній практиці, так і у науковій та навчальній літературі. Таке сусідство понять іноді вносить неясність і плутанину у визначення функцій цих осіб, тому необхідно з'ясувати «хто є хто».

Бізнес (англ. business) – це підприємницька діяльність, справа або заняття, що є джерелом одержання прибутку. **Підприємець** як дрібний власник виконує свої функції самостійно, особистою працею створює продукти (послуги), приймає необхідні рішення в процесі розвитку своєї справи, сам забезпечує виробничу діяльність, реалізує продукцію і привласнює результати власної праці.

1) **Аудитор – не диктатор**, а мотиватор поліпшення**.**
2) Підрозділи, що перевіряються, не повинні боятися аудиту.
3) Аудитор повинен допомагати тим, кого перевіряє, розпізнавати проблеми і домагатися усунення їх причин.
4) Діалог повинен сприяти поліпшенням.
5) Аудитор повинен чітко уявляти цілі підрозділу.
6) Задокументовані процеси СМІБ.

Кращий посібник для переліку питань з аудиту – це опис процесу.

7) Результати аудиту повинні документуватися.
8) Процеси СМІБ повинні бути перевірені на:
   a) досягнення цілей відповідно з заданими значеннями процесів;
   b) актуальність заданих значень;
   c) ефективність заходів для досягнення цілей.
9) Аудит повинен передбачати постійне відстежування виявлених проблем.

Принципи проведення аудиту.

Принцип 1: Етика поведінки – основа професіоналізму.

Довіра, прямота, конфіденційність і стриманість – обов'язкові умови при проведенні аудиту.

Принцип 2: Уміння представляти матеріал неупереджено, правдиво і точно.

Висновки і звіти про аудит повинні правдиво і точно відображати діяльність під час перевірки. Необхідно повідомляти про основні труднощі, неврегульовані або ті, думки щодо яких не збіглися в аудитора і тих, кого він перевіряв.

Принцип 3: Належна професійна сумлінність – ретельність і здатність давати оцінку.

Відповідно до виконуваних завдань і довіри, що надаються замовником аудиту.

Принцип 4: Незалежність – основа неупередженості.

Аудитори є незалежними від об'єктів діяльності, вони вільні від упереджень і зіткнень інтересів.

Принцип 5: Підхід, заснований на свідченнях (фактах).

Аудитори засновують свої висновки тільки на фактах. Свідчення з аудиту можна перевірити.

Виявлено невідповідностей:
з них значних:
незначних:
П.І.Б., підпис аудиторів:

Дата:

+ Протоколи невідповідностей

Журнал реєстрації звітів про аудити

Порядковий номер звіту	Підрозділ, що перевіряється	Дата аудиту	П.І.Б. аудиторів	Копії звіту направлені:	Помітка про усунення невідповідностей
1	2	3	4	5	6

а) Керівництво підрозділу, що перевіряється, повинно забезпечити вчасне виконання коригувальних дій (без невиправданих затримок), щоб усунути виявлені невідповідності та їх причини.

б) Аудитори повинні перевірити виконання і ефективність виконаних коригувальних і попереджувальних дій, і зробити позначку про результати перевірки.

в) Якщо коригувальні дії не виконані або недостатньо ефективні, аудитор відзначає це у бланці невідповідностей.

г) Керівник підрозділу визначає нові коригувальні дії та / або терміни по їх виконанню, після чого слідує чергова перевірка.

д) Якщо підрозділі, що перевіряється, не будуть усунені невідповідності в повторно призначені терміни, аудитор доводить до відома про це представника керівництва по системі для прийняття відповідних заходів.

Алгоритм усунення невідповідностей

1) Визначити «видиму» причину відмови в системі.
2) Визначити причину потенційної невідповідності.

Відхилення – лише симптоми серйозних причин, необхідно з'ясувати справжню причину, щоб розпізнати реальні масштаби проблеми і визначити потенціал для поліпшення.

3) Визначити коригувальні дії (КД).
4) Визначити превентивні дії (ПД).
5) Виконати КД і ПД (за необхідності).
6) Контроль виконання та ефективності КД і ПД.

9 Заповідей успішного проведення аудиту

Справа виглядає інакше, коли зростають масштаби виробництва, організуються філії, дочірні компанії, підприємство виходить зі своєю продукцією за рубіж. Власної праці підприємця стає недостатньо. Кожна з функціональних сфер роботи підприємства стає самостійним напрямком, тобто відбувається поділ функцій на виробничі і управлінські, що вимагає професійного підходу до керування. Ось тут і з'являється на ринку праці робоча сила відповідної спеціальності – **професійний менеджер**.

Звісно, підприємець як власник може і сам вирішувати питаннями управління, не приймаючи участь у безпосередньому виробництві. У цьому випадку підприємець (бізнесмен) і менеджер поєднуються в одній особі. Це характерно в основному для малого бізнесу. Але багато середні, за певними критеріями, підприємства та усі великі, як правило, управляються найманими професійними керівниками – менеджерами.

Під управлінням бізнесом прийнято мати на увазі управління комерційними і господарськими організаціями. Поряд з поняттям «управління бізнесом» застосовують термін «ділове адміністрування». Якщо мова йде про державне підприємство (організацію), то застосовують термін «державне управління». Отже, підприємець (бізнесмен) і менеджер – це близькі поняття, але не те саме. **Бізнесмен – це власник**, що використовує свій або позиковий капітал з метою одержання прибутку або підприємницького доходу. Він може не займати у своєму підприємстві ніякої офіційної посади, але може входити в його правління або наглядову раду.

Слово «менеджер» має кілька значень:

1) найманий професійний управляючий;
2) фахівець із управлінням виробництвом;
3) підприємець у професійному спорті тощо.

Таким чином, менеджер – це найманий робітник, що займає певну посаду в даній організації. У той же час менеджер у ряді випадків може бути співвласником цього підприємства, мати його акції. У роботі менеджера і бізнесмена є загальні риси: обидва переслідують цілі, поставлені перед підприємством; застосовують певні способи управління; планують, координують і контролюють діяльність працівників підприємства; працюють на свій страх і ризик. Один ризикує своєю посадою, другий – власним капіталом.

Сьогодні виник значний суспільний інтерес до менеджменту та вивчення управлінського досвіду в закордонних країнах, де він уже давно й широко застосовується та належним чином поставлена підготовка професійних керуючих, які відповідали б потребам ринкових відносин. Центром наукових досліджень і підготовки професійних керівників, безумовно, є США, як родоначальник менеджменту. Це країна з найбільш розвиненою системою управління, яка вимагає постійного притоку все нових і нових сил. Так, наприклад, широке наукове дослідження та практичну підготовку менеджерів проводять Гарвардська школа бізнесу, Стенфордська школа бізнесу, Слоунівська школа в Массачусетському технологічному інституті, Школа бізнесу Мічиганського університету та ін. Всього в країні налічується понад 1300 навчальних закладів. Саме у США публікується найбільша кількість наукової і навчальної літератури з менеджменту.

У європейських країнах проблемам менеджменту також приділяється значна увага. Створено провідну європейську асоціацію EFMD[1] (Європейський фонд розвитку менеджменту), куди входять близько 300 центрів навчання менеджерів. У програмах цих шкіл велике значення надається вивченню практичних дисциплін з різних видів виробничої діяльності, міжнародних проблем бізнесу та управління, а також соціологічним питанням.

У Японії система підготовки менеджерів побудована інакше. Великі фірми самі ведуть підготовку керівників, тобто відбувається навчання досвідом, коли старші за посадою вчать молодших. Так, у країні прийнято, що на підприємствах навчаються усі – від робітника до керівника фірмою.

Наукові основи менеджменту

Відоме положення, **що наука – це безпосередньо продуктивна сила**, підтверджується корінними якісними перетвореннями у техніку, технології та процесі виробництва. Управління в таких умовах неминуче веде до необхідності наукового підходу, ефективно-

[1]**EFMD** (European Foundation for Management Development) – Європейський фонд розвитку менеджменту, штаб-квартира якого розташована в Брюсселі, представляє інтереси бізнес-шкіл і коледжів, які викладають менеджмент, а також регулює питання, пов'язані з навчанням менеджменту і подальшим розвитком цих організацій. До фонду EFMD можуть увійти як школи бізнесу, так і комерційні компанії.

ТОВ «ХХ»		
БЛАНК НЕВІДПОВІДНОСТЕЙ		
Місце перевірки: Служба управління ІТ	**№ пункту ISO, СТП** п.А. 12.3 ISO 27001	**Дата:** 14.11.2018
		Номер 3
НЕВІДПОВІДНІСТЬ Відсутня політика резервного копіювання. Створення резервних копій не виконується на вузлах М5.М3.М5.		
Аудитори		**Відповідальна особа**
1.Іванов І.Т.	*2.Петренко П.Т.*	*Сидоренко А.П.*
КОРИГУВАЛЬНІ / ПОПЕРЕДЖУВАЛЬНІ ДІЇ, ПРИЙНЯТІ ДЛЯ ВИПРАВЛЕННЯ НЕВІДПОВІДНОСТІ 1. Розробити політику резервного копіювання 2. Розробити і виконувати графік резервного копіювання **ТЕРМІН ВИПРАВЛЕННЯ: 24.11.2018**		
ПЕРЕВІРКА ЕФЕКТИВНОСТІ ВИКОНАННЯ КОРИГУВАЛЬНИХ ЗАХОДІВ Додатковий аудит через 3 міс. з метою підтвердження здійснення резервного копіювання.		
Незадовільне виконання коригуючих дій **ПІДПИС: _____ ДАТА: _____**	**ЗАДОВІЛЬНЕ ВИКОНАННЯ КОРИГУЮЧИХ ДІЙ** **ПІДПИС:** Петренко П.Т. **ДАТА:** 25.11.2018	

Приклад звітності з внутрішнього аудиту.

Акт № _____ від _____ про здійснення внутрішньої перевірки

_____

Протокол коригувальних та запобіжних дій за результатами внутрішньої перевірки підрозділу _____ (акт № ____ від _____)

Фрагмент вимог процедури з внутрішнього аудиту. Приклад.

Затверджую
_____Ф.И.О.
_____ 20___ г.

ЗВІТ №
про проведення внутрішнього аудиту
_____
(найменування підрозділу)

Приклад: *«Тільки одна людина з відділу по роботі з клієнтами не знайома з правилами з ІБ. Хоча весь відділ пройшов навчання відповідно до графіку».*

«Критичне відхилення» – коли повністю або у більшості випадків не дотримуються вимоги одного або декількох елементів системи менеджменту.

Наприклад: *«Немає процедури та робочого процесу резервного копіювання інформації» – повністю не дотримуються вимоги ISO 27001. Пункт А. 12.3*

Що таке некритичне відхилення?

«Некритичне відхилення» – коли вимоги елемента якості виконуються не в повному обсязі, але відхилення не може спричинити помітних негативних наслідків

Наприклад, *якщо був встановлений факт, що 1 раз з 15 згідно графіка не було вироблено резервне копіювання.*

Реєстрація відхилень. Коментар.

Класифікація невідповідностей на **критичні – не критичні, істотні – несуттєві** вимагає чіткої вказівки в процедурі з проведення внутрішнього аудиту про те, як аудитор повинен оцінити і класифікувати невідповідність.

Фрагмент вимог процедури з внутрішнього аудиту (див. рис. 5.10).

Приклад:

Якщо аудитор виявляє критичне відхилення, він повинен повідомити про даний факт керівнику підрозділу для оперативного усунення порушення.

На кожне виявлене відхилення заповнюється окремий бланк.

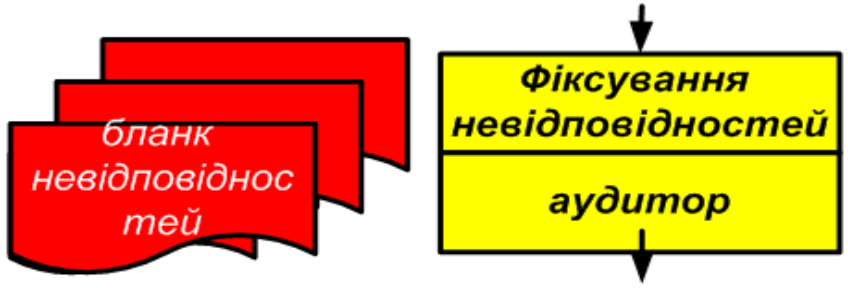


Рис. 5.10. Фрагмент вимог процедури з внутрішнього аудиту

му використовуванню всього нового та передового. Із середини XX ст. відбувається різке прискорення науково-технічного прогресу, що зробив вплив не тільки на науку і техніку, але і на всі сторони громадського життя. Зросли вимоги до рівня підготовки фахівців, їхньої кваліфікації; культурного рівня; можливості швидко відновлювати свої сили, витрачені на роботі в умовах стресових ситуацій; керування складними системами та пристроями; роботи в зонах підвищеної небезпеки, радіації та ін. **Ділова активність стала неможливою без міцного і ефективного зв'язку між наукою, технікою та управлінською діяльністю людей.** Значно зріс ступінь відповідальності керівників за результати своєї праці. Управління виробничими процесами піднялося на новий рівень, коли людина стала керувати не тільки діями машин і механізмів, але і цілими системами, що управляють цією технікою.

Історично розвиток управлінської науки в нашій країні був обумовлений і здійснювалося в умовах панування суспільної форми власності, директивних методів керівництва без належного обліку дії ринку, конкуренції і взаємодії різних видів і форм власності, характерних для західного світу. Суспільство не змогло належним чином використати величезне багатство вітчизняної управлінської науки з метою поліпшення народного господарства, країна прийшла до дефіцитної економіки, а в 90-х рр. – до кризи.

По-іншому складався процес становлення і розвитку науки управління – менеджменту – у країнах Заходу і Японії. Науковий інтерес до менеджменту різко зріс у зв'язку з найгострішими економічними кризами, депресією, фінансовими потрясіннями та жорстокою конкурентною боротьбою. Великі господарські структури були зацікавлені в таких наукових розробках, які відповідали б потребам практики, допомагали б ефективно управляти, передбачати хід розвитку економічної ситуації, зробили б так, щоб працювала формула «витрати – вигоди» тощо.

Наукові праці з питань управління, написані раніше, починаючи з Ф. Тейлора[2], А. Файоля[3] і більш пізніх – М.П. Фоллет[4], Е. Мейо[5],

[2]**Фредерик Уинслоу Тейлор** – (1856 – 1915 рр.), засновник наукового менеджменту, не лише заклав теоретичні основи, але і зробив справжній переворот в управлінні виробництвом. Пропагував активне управління виробництвом, суть якого бачив в тому, щоб робота кожного виконавця планувалася заздалегідь. Уміння ставити і реалізовувати цілі Тейлор визначав як «мистецтво точно знать, що і як необхідно зробити найкращим і найбільш дешевим чином».

у яких були сформульовані головні напрямки роботи керівника підприємством та інші управлінські питання, вже до початку 30-х рр. не влаштовували великих промисловців і банкірів [3]. У США після Другої світової війни значно активізувалася діяльність вчених з проблем управління. Була створена так названа безприбуткова науково-дослідна корпорація «РЕНД корпорейшн[6]», яка обслуговувала науковими розробками військове відомство і великі монополії, а також економічна рада при президенті. Вчені ряду університетів та інших вищих навчальних закладів за замовленням уряду і великих фірм розпочали проводити дослідження проблем управлінської праці. Вийшли великі фундаментальні та прикладні роботи американських вчених – економістів, соціологів і психологів з питань менеджменту. Визначилися і основні напрямки цих досліджень. На високому науковому рівні були розроблені питання стратегічного управління та планування, інноваційний менедж-

[3] **Анрі Файоль** – (1841 – 1925 рр.), французький гірський інженер, підприємець, теоретик і практик менеджменту, засновник адміністративної (класичною) школи управління. Уперше в історії науки управління розглядав менеджмент системно, аналізуючи його за функціональними ознаками, включаючи оперативне планування, календарне регулювання, управлінську координацію і контроль, з організацією зворотного зв'язку; визначив принципи менеджменту.

[4] **Мері Паркер Фоллетт** – (1868 – 1933 рр.), «філософ» бізнесу і управління, визначила менеджмент як забезпечення виконання роботи за допомогою інших осіб; проаналізувала стилі керівництва і розробила теорію лідерства. Внесла видатний внесок у розвиток ідей, пов'язаних з природою влади, необхідністю координації зусиль, вирішенням конфліктів і структурою організацій, націлених на забезпечення максимальних можливостей для спільних (корпоративних) зусиль.

[5] **Елтон Джордж Мейо** – (1880 – 1949 рр.), відомий американський психолог і соціолог; дослідник проблем організаційної поведінки і управління у виробничих організаціях; один з основоположників індустріальної соціології. Заснував рух «за розвиток людських відносин»; один з основоположників школи людських відносин. Відомий як непримиренний критик положень класичної школи менеджменту, що відкидає її орієнтацію на пріоритет формалізації стосунків і ієрархічної будови організації, а також як автор гуманістичної соціальної філософії, багато в чому альтернативної тейлоровским уявленням про природу людини і запропонованим ним методам управління.

[6] **Корпорація РЕНД (RAND)** – всесвітньо відомий американський стратегічний центр і перша у світі організація, яку стали називати «фабрикою думки». «Проект РЕНД», переріс ший потім в «РЕНД корпорейшн», заснований у кінці 1945 р. генералами армії у рамках Авіаційної компанії «Дуглас» в Санта-Моніці (Каліфорнія, США) в цілях охорони національної безпеки країни. У травні 1948 р. РЕНД почав самостійне існування, ставши незалежною, приватною, некомерційною, позапартійною організацією. Одним з основних завдань Ренду залишається забезпечення національної безпеки США шляхом проведення досліджень і аналізу найбільш гострих проблем, що стоять перед американським суспільством.

«Відсутня процедура і не виконується робота по перевірці ІС на предмет безпеки перед впровадженням на виробництво».

Формулюємо мовою процедур СМІБ, ISO 27001.

2) Посилання на факти.

Потрібні тільки факти. Повідомлення про них повинні бути точними

Приклад:

«Відсутній гриф «Таємно» на документі «Стратегічний план розвитку 2019» від 12.11.2018. Документ входить до переліку документів під грифом «Таємно». Згідно з процедурою 5.1-05 повинен маркуватися.

3) Де відхилення було виявлено.

Заява повинна точно ідентифікувати, де воно було виявлено.

Приклад:

«Сектор закупівлі обладнання ВМТП»

«Відділ по роботі з персоналом»

«Управління ІТ»

«ЦПУ цеху №1"

Для чого потрібна така ідентифікація?

4) Дату виявлення відхилення.

Посилання на вимогу процедури СМЯ, ISO 9001.

Приклад:

«п.7.5 ISO 27001»

«п.4.3 СТП 4329-97»

«п. 1.2 Положення про конфіденційність »

Як оцінити серйозність відхилень?

– Аудитор повинен бути в змозі відрізнити серйозні відхилення від менш серйозних.

– Є два питання, які допомагають зрозуміти серйозність відхилення:

Які небажані наслідки можуть мати неусунені недоліки?

Яка ймовірність цих небажаних наслідків?

Що таке критичне відхилення?

«Критичне відхилення» – коли часткове невиконання вимог елемента ІБ має серйозні наслідки.

– вивчення процесів і документації;
– складання анкетування\переліку дій;
– складання плану.

Отримання об'єктів свідчень.

В ході перевірки аудитор запитує представника відділу, як виконується та чи інша операція, і підтверджує сказане перевіркою зразків або в ході бесіди з іншою особою, тому:

Місце перевірки – «там, де йде робота».

Можливі причини появи відхилень.

– Розглянуті документи не містять вимог щодо ІБ.
– Вивчені процеси (документи, записи СМІБ) не відповідають вимогам процедур СМІБ або вимогам стандарту ISO 27001.
– Документи не застосовуються на практиці або не дотримуються їх обов'язкові вимоги.
– Прийнята практика неефективна, тобто необхідні результати не досягаються.

Що таке відхилення?

Умова, що надає шкідливий вплив на інформацію (інформаційні активи) – **порушення вимог СМІБ**. (Втрата однієї або декількох властивостей ІБ).

Фіксування невідповідностей.

Факти відхилень повинні бути узгоджені до того, як аудитори покинуть зону аудиту і прямуватимуть в іншу.

Заява про відхилення **повинна бути зрозумілою за змістом** як учасникам аудиту, так і тим, хто не брав участі в ньому.

Примітка. *У промисловості прийнято надавати власні назви деяким видам діяльності, документам і т.д. Слід використовувати цю термінологію.*

Заява про відхилення повинна містити:

1) Що саме було виявлено.

Необхідно чітко вказати: який аспект є невідповідним (яка вимога була порушена).

Приклад:

«Умови зберігання інформації в архіві _____ не відповідають вимогам З 777 5.8.2-03 ....».

«Створення резервної копії не проводиться в задані в « Положенні про резервне копіювання ... » терміни.

мент, адміністративний і кадровий менеджмент, фінансовий менеджмент т.ін. Розроблені теорії ігор, теорія систем і системного аналізу, теорії мотивації, моделі лінійного програмування, принципи керування гнучкими автоматизованими системами, принципи та методи проектування організацій тощо. Такі ж, але в іншому масштабі наукові дослідження і розробки проводилися у Великобританії, Німеччині, Франції та інших економічно розвинених країнах. У Великобританії, наприклад, була заснована найбільша наукова організація країни – Науково-дослідна рада, створений Лондонський інститут стратегічних досліджень, а також центри економічних досліджень у Лондонському та інших університетах і вищих навчальних закладах. Розробки і дослідження, створення теорій управління, концептуальний підхід до питань управління в США створили необхідні умови і з'явилися основою для формування нової науки – менеджменту.

Предмет менеджменту як науки визначився історично порівняно недавно – у середині XX ст., однак його методологічні джерела беруть початок з минулого. Менеджмент увібрав у себе наукові основи управління і результати управлінської діяльності багатьох поколінь людей. Процес керування мав місце завжди, як тільки виникло людське суспільство. В античних джерелах, що дійшли до нас («Політика» Аристотеля, «Про сільське господарство» Колумелі тощо) і у ряді інших, більш пізніх роботах римлян висловлюються погляди на управління і юридичні норми, правила і принципи у відносинах «керівники – керовані». З розвитком цих поглядів змінювався зміст управлінських підходів: починаючи від визнання справедливості рабства і управління рабами, до пізніших підходів, заснованих на ідеях християнства, що засуджували рабське приниження і які проповідували рівність у відносинах між людьми.

У середньовіччі основи управління описані в працях релігійних діячів, ченців, що організували достатньо розвинуте на той час сільськогосподарське виробництво і ремесло. Однак управління, засноване на позаекономічному примусі, не відповідало ринковим відносинам і найманому характеру праці. Виникли ідеї, які називають утопічними, де керування виробництвом мислилося на основі справедливого розподілу та рівності його учасників. Томас Мор, Томма-

зо Кампанелла, Роберт Оуен[7] та інші намагалися обґрунтувати принципи і методи такого керування.

Подальший період суспільного розвитку висунув цілу плеяду дослідників сутності нових економічних явищ, ринкових відносин, у тому числі і проблем управління виробництвом, які з'явилися, нових поглядів на відносини керуючого і керованих, панування та підпорядкування. Розвиток нових відносин власності – відносин власника засобів виробництва і найманого робітника, привело до появи проблем, без рішення яких виробнича діяльність найчастіше не приносила бажаних результатів. Протиріччя між найманими робітниками і власниками капіталу вели до неминучих економічних втрат і соціальних потрясінь. Вихід з такого положення керівники, як практики, так і теоретики, почали шукати в удосконалюванні відносин розподілу, більш ефективних принципів стимулювання праці, зміні форм його оплати, ціни праці, кращої організації виробничого процесу, навчанні робітників більш інтенсивним і продуктивним прийомам і методам виконуваної роботи та інших способів згладжування виниклих протиріч. У таких умовах **праця керівника стала здобувати усе більш науковий характер**, вимагала експериментів, обміну досвідом, наукової оцінки управлінських рішень та інших наукових досліджень із наступною перевіркою їх на практиці. Виник новий, науковий підхід до керування, що одержав назву **тейлоризм** – названий ім'ям його засновника американського інженера Ф. Тейлора. Широке застосування ідеї тейлоризму знайшли в роботі великих американських підприємств, поширилися по всіх європейських країнах. У результаті їхнього використання в управлінні виробництвом був зроблений перший крок у становленні менеджменту як науки.

Разом з тим період становлення менеджменту збігся з розвитком нового напрямку в економічній науці – неокласичним. У роботах вчених цього напрямку велика увага приділялася проблемам економічної практики, ролі ринку в економіці, утворення ціни товару, як співвідношення попиту та пропозиції, концепції факторів виро-

[7] **Роберт Оуен** – (1771 – 1858 рр.), англійський соціаліст-утопіст; намагався здійснити свої соціалістичні ідеали за участю самих робітників. Оуен розрізнив в продуктивних силах, що розвивалися при капіталізмі, передумови вищої організації суспільства, пов'язаної зі встановленням суспільної власності на засоби виробництва.

Рис. 5.8. Карта процесу

Анкетування\переліки питань постійно приводиться у відповідність до вимог підприємства (див. рис. 5.9).

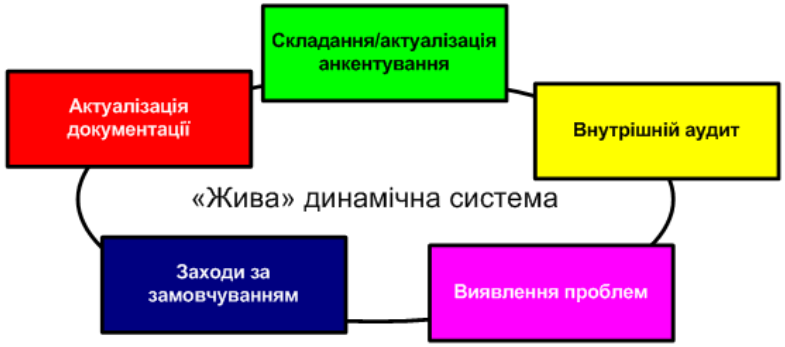


Рис. 5.9. Процес складання анкет

4) Заключна нарада.
5) Підготовка звітності по аудиту.
6) Перевірка виконання коригувальних / превентивних дій.
7) Помітка про виконання.

Хороший аудитор – це підготовлений аудитор.

1) Підготовка до аудиту:

Модель процесу (див. рис. 5.7, 5.8) – джерело питань для анкетування \ переліку питань внутрішнього аудиту.

Етапи аудиту на місці

1) Підготовка до аудиту (вивчення процесів і документації, складання анкетування і планів).

2) Вступна нарада.

3) Проведення аудиту (інтерв'ю, спостереження за роботою, збір і оцінка об'єктивних свідчень, реєстрація відхилень, ведення заміток).

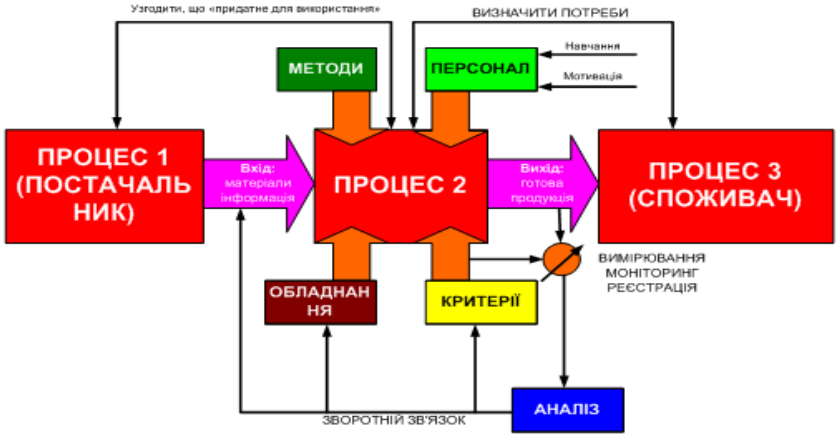


Рис. 5.7. Модель процесу

бництва, суб'єктивним оцінкам матеріальних благ, волі їхнього вибору та інших економічних явищ. Все це також стало складовою частиною методологічних основ менеджменту.

Значний вплив на проблеми управління і їхнє теоретичне узагальнення зробили ідеї кейнсіанців, які досліджували можливості державного регулювання економіки з використанням економічного механізму і адміністрування, регулювання попиту та пропозиції шляхом втручання держави в ринковий механізм т. ін. [4, 5]. Цими ідеями та теоріями в менеджменті керувалися аж до середини XX ст. Надалі основними напрямками керування стали теорії найбільш прагматичні, націлені на рішення наступних проблем:

- управління в концернах і великих фірмах;
- психологічний клімат у робочих колективах;
- робота з кадрами;
- мотивація праці та питання людських відносин;
- організація праці та ін.

Багато **досліджень**, які проводилися в 60-ті рр. **на основі системного аналізу і теорії інформації, принципів стратегічного менеджменту, системного та ситуаційного підходів до аналізу внутрішніх і зовнішніх змінних організацій, концепції корпоративної культури, проблем міжнародного менеджменту** підтверджують, що менеджмент – це самостійна наука, що має методологічні основи, свій предмет і метод.

Як і всяка інша наука, менеджмент містить властиві тільки йому категорії і наукові поняття, що відбивають сутність управлінської праці. До них відносяться:

- управління – як процес впливу на працівників в інтересах досягнення поставлених цілей;
- об'єкт управління – люди, техніка і технології, підприємство та ін.;
- суб'єкт управління – особистість або кібернетичний пристрій;
- організація як сфера діяльності менеджера;
- планування, координація, мотивація і контроль;
- стиль управління та ін.

У процесі наукових досліджень управлінських проблем вченими були відкриті і обґрунтовані об'єктивні закони життєдіяльності

організацій і закономірності, характерні для управлінської праці. Серед них закони: пропорційності і планомірності, адміністративної ємності, ритму робіт та ін. У менеджменті, як науці виокремилися відповідні розділи:

- методологічні основи наукового управління;
- організаційні і управлінські структури;
- функції управління;
- процес управління, кадровий менеджмент;
- стратегічне управління, інноваційний менеджмент;
- управління міжнародною економічною інтеграцією та ін.

Менеджмент як практика управління включає: керування виробництвом, керування маркетингом, керування фінансовою діяльністю, керування кадрами, облік, контроль і аналіз господарської діяльності. Дані питання складають предмет навчальних дисциплін з менеджменту, входять у навчальні програми, розглядаються на прикладах конкретних ситуацій. Тут простежується прямий зв'язок теорії і практики.

Таким чином, **предмет менеджменту** як науки управління охоплює дослідження законів і закономірностей життєдіяльності організацій і відносин між працівниками в процесі керування. Менеджмент, як і будь-яка інша наука, має свій особливий метод дослідження явищ управлінської діяльності.

В основі методу менеджменту лежить діалектичний підхід, що дозволяє розглядати управлінські проблеми в їхньому постійному взаємозв'язку, русі та розвитку. Це означає, що явища вивчаються від простого до складного, від нижчого до вищого, від конкретного до абстрактного, від старого до нового та ін. У центрі досліджень у менеджменті перебуває людина, що здійснює продуктивну діяльність, будь то керівник або виконавець. Але одна людина завжди пов'язана з іншими людьми, вона працює в колективі, є членом організації (підприємства, установи, фірми тощо), тому метод менеджменту – це науковий аналіз поводження людини в організації, взаємозв'язок і взаємний вплив людини та організації. Особливо важливим у менеджменті є метод системного аналізу, що затвердився в середині XX ст. Йому передувало створення системи математичної логіки (У. Джевонс та Э. Шредер), а надалі розробка методу лінійного програмування, виникнення кібернетики як науки про

а) Чи документовані функції вашого відділу та обов'язки співробітників? Покажіть.

Таблиця 5.2. Приклад анкетування для внутрішнього аудиту. Результат заповнення анкетування.

N пункту РК, СТП, ISO 27001, Інструкції	**Контрольні питання (Вимоги)**	**Відповідність / невідповідність вимогам**	**Спостереження за роботою, переглянуті документи, записи, інтерв'ю**
п.8 ISO 27001, п.4.6 СТП 6-2003	Як здійснюється забезпечення ресурсами запланованих заходів щодо зниження ризиків? Покажіть.	Відпов.	СТП 5_06-2003- Забезпечення ресурсами Наказ N9 34 від 16.04.2018 на фінансування робіт із забезпечення безпеки

Складено _____
Дата _____

б) Назвіть цілі Вашого відділу в області забезпечення безпеки?

в) Як Ви розумієте свою роль в Політиці ІБ?

г) Якими документами з безпеки (внутрішніми і зовнішніми) керуються підрозділи в роботі? Чи є їх перелік?

д) Які Ваші основні правила з безпеки? Покажіть.

е) Як зберігається конструкторська і технічна документація? Покажіть правила.

ж) Хто має право на вхід в архів з документацією? Де це регламентовано?

з) Які проблеми у Вас існують з документацією?

и) Які існують проблеми з документацією в електронному вигляді?

к) Як давно Вам міняли пароль на вхід в ІС?

л) Як давно Ви проходили навчання з ІБ?

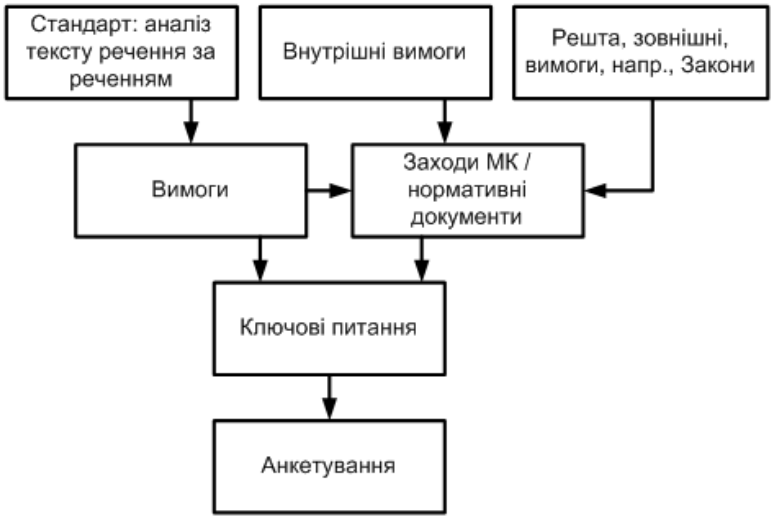


Рис. 5.6. Алгоритм розробки анкети

Таблиця 5.1. Приклад анкетування

Завод / Підрозділ: Кер.	Місце знаходження:	Дата: 20.01.2018		Аудитори: 1. 2.
№ п/п	Питання аудиту	Вимога СМІБ		Зауваження
		документована	виконана	
1	Викладена політика в області ІБ вищим керівництвом в письмовому вигляді і відома вона на всіх рівнях?	Так	так	
2	Чи задокументована система менеджменту ризиків?	частково	так	
2.1	Чи проводиться аналіз ризиків?	ні	частково	

Приклад анкетування\переліку запитань для внутрішнього аудиту у технічному відділі.

керування складними динамічними системами. В результаті відкриттів вчених в області системного аналізу з'явилася можливість застосовувати на практиці управління, математичні моделі і використовувати метод математичного моделювання.

Види і функції менеджменту

Розгляд наукових основ менеджменту дозволяє зробити висновок, що управління стосується всіх видів продуктивної і суспільної діяльності людини. Вона управляє, насамперед, собою, своїми діями, емоціями, поведінкою тощо. У побуті та на виробництві людина управляє приладами і механізмами, а також діяльністю інших людей. Однак у той же час вона сама є об'єктом керування. Види управління поділяються за ступенем складності. Наприклад, управління групою людей, зайнятих збиранням овочів, і управління комп'ютерною технікою або інформаційними системами значно відрізняються за ступенем складності, спеціальності і кваліфікації керівників.

Усі види управлінської діяльності перелічити тут неможливо, але деякі з них, що мають для менеджменту найбільш важливе значення, назвати необхідно. Зведемо їх у кілька груп, у кожній з яких є загальні напрямки управлінської діяльності. Одним з таких видів є **господарське управління**. Воно включає управління виробничою, маркетинговою, фінансовою і кадровою службами в державному та приватному підприємствах (організаціях).

Тісно пов'язане із цим видом **технічне управління**, до якого належить керування технікою і технологіями; ремонт і профілактика машин, технічних пристроїв і механізмів; заміна застарілої техніки та технології; навчання персоналу прийомам і методам роботи; наукова організація праці і ряд інших питань.

У всіх організаціях, де має місце колективна праця, виникла необхідність ще одного виду управлінської діяльності – **управління соціально-психологічними питаннями спільної діяльності людей**. На виробництві з'явилися фахівці – соціологи та психологи, об'єктом роботи яких став морально-психологічний клімат у колективі, психологічний стан окремих працівників, рішення соціальних питань, організація відпочинку, підвищення культурного рівня працюючих т. ін.

Однак підприємства не ізольовані від зовнішнього оточення, вони пов'язані з діяльністю державних, суспільних і міжнародних органів та організацій. Це зовнішнє середовище має свої види управління: **державне управління, управління громадськими організаціями та ін.**

У сфері матеріального виробництва характерними є наступні види управлінської роботи:

– **управління виробництвом** – вибір основних параметрів роботи техніки і застосування технологій, визначення обсягу випуску продукції або надання послуг, розміщення людей, організація подачі матеріалів і комплектуючих виробів, інструментів, технічної документації, обслуговування та ремонт машин і механізмів, контроль якості т. ін.;

– **управління поставками і збутом** – укладання договорів на поставки та збут, організація зберігання, упакування, сортування та роботи транспортних засобів, ведення обліку і контролю. Сюди ж необхідно віднести і управління маркетингом, що здійснює вивчення ринків збуту та поставок сировини, матеріалів і енергії, кон'юнктуру ринку, створення цінової політики і організація реклами;

– **управління фінансовою діяльністю** – формування і розподіл фінансових ресурсів, складання бюджету та фінансового плану, формування портфеля інвестицій, оцінювання поточного і перспективного фінансового стану організації, робота із кредиторами т. ін.;

– **управління кадрами** – рішення питань підбора, розміщення і навчання працівників, поліпшення умов їхньої праці та відпочинку, управління соціально-психологічними процесами, створення необхідного морально-психологічного клімату на підприємстві, організація роботи із профспілками у вирішенні трудових суперечок і конфліктів;

– **управління інноваціями** – організація процесу наукових і дослідно-конструкторських робіт і розробок, використання у виробництві нової продукції або послуг, нової організації виробництва та управління.

Ці види і напрямки управлінської діяльності реалізуються та проявляються в її **функціях**. У менеджменті сформульовані і об-

3) розробити загальний план аудитів.

Як скласти програму аудитів на рік? Приклад.

Затверджую: _____

Елементи ISO 27001 / Підрозділи	П.І.Б. призначених аудиторів	4.2.1 .... 4.2.2 5.1 5.2.1...	7.1	7.2..	8.3	A 5	A 6	A 7	A 8	A 9	A ...	A 14	A 15	A 16	A 17	A 18	Дата
Служба збуту		X															1
Відділ постачання		X	X					X									2
Технічний відділ		X															3
Служба якості		X		X	X					X							4
Ділянка прийняття сировини		X		X	X							X					5
Ділянка синтезу		X		X	X							X					8
Ділянка пакування		X		X	X								X				11
Склади		X															2
ЦЛМ		X		X										X			1

План проведення аудиту

Підприємства _____(Конкретний аудит в задані терміни)

Логотип	Графік проведення аудиту		Звітний рік діє до: 2020
			Лист 1 з 2
Аудитор 1 К. Мустерманн	Аудитор 2: І. Байшпіль	Дата: 2.6.2019	Аудит системи

Час, год.	Підрозділи	Учасники бесіди	Елементи
9.00 -9.30	Служба безпеки	Гінц, Кунц, Леманн	4, A5-A18
9.30-11.30	Керівництво	Гінц, Кунц	5, 6, 7
11.30-13.30	HR	Шмідт	5, A8
14.30-15.30	Служба охорони	Обговорення аудиту аудиторами	A11
15.30-17.00	IT	Леманн	A7, A9-A18
17 00	Заключна бесіда	Все	

Запорука успіху аудиту – анкетування (див. рис. 5.6, табл. 5.1, 5.2).

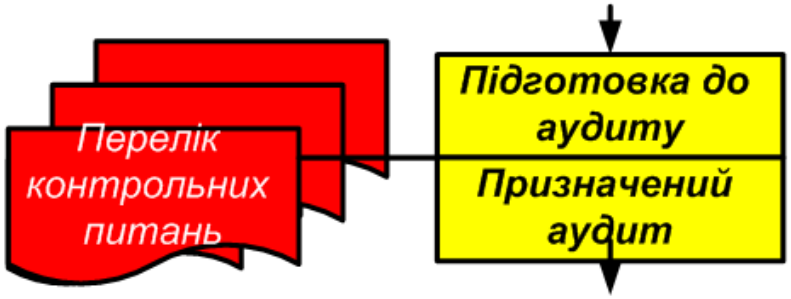


Рис. 5.4. Підготовка до аудиту

Лідер групи аудиторів несе відповідальність за планування аудиту (див. рис. 5.5):

– узгодження дати;
– складання плану;
– призначення індивідуальних завдань;
– підготовку звітності по аудиту;
– аудит на адекватність;
– організацію нарад аудиторів (при необхідності);
– подання групи аудиторів і проведення вступної та заключної нарад.

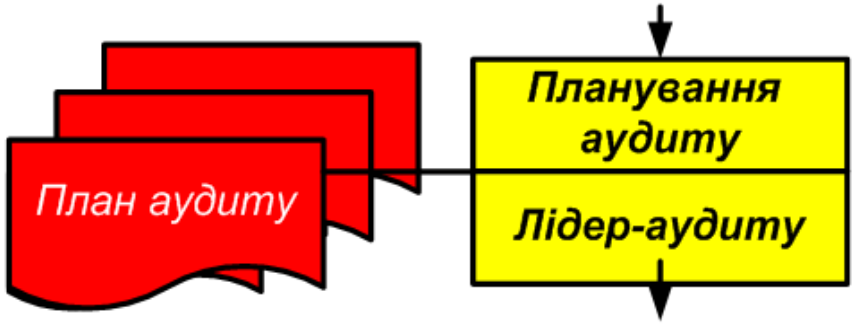


Рис. 5.5. Планування аудиту

Планування аудитів

Три етапи планування аудиту:

1) скласти методичну інструкцію з планування і проведення внутрішніх аудитів;

2) визначити цілі і обсяг аудитів;

ґрунтовані кілька основних функцій. Головною з них є **планування**. У процесі планування менеджер визначає цілі та завдання підприємства, необхідні для їхнього рішення матеріальні, фінансові і трудові ресурси та резерви, встановлює строки реалізації поставлених цілей, відповідальних за їхнє виконання та самих виконавців. Планування дозволяє менеджерові діяти усвідомлено, керуючись як довгостроковою перспективою, так і проблемами, що виникають у поточній роботі.

Наступна функція менеджменту – **організаційна.** Спланові дії необхідно втілити на практиці, організувати їхнє виконання. Ця робота пов'язана зі створенням самої організації, її структури, управління і комунікацій, а також із забезпеченням роботи людей всіма необхідними засобами, документацією і інформацією. Це рішення широкого кола питань виробничого процесу, поставок і збуту та ін. Під час організації як процесу виникає необхідність корегувати роботу людей, координувати їх зусилля, забезпечувати необхідний ритм і послідовність виконання трудових операцій. У цьому зв'язку **координація** є також функцією менеджменту. Організовуючи і координуючи роботу підлеглих, менеджер постійно зіштовхується з різним відношенням людей до своєї (дорученої) справи. Люди працюють із різною інтенсивністю і продуктивністю, можуть проявляти ініціативу та старання, а можуть працювати «від і до». Виникає необхідність у наступній функції – **мотивації.**

І, нарешті, будь-яка робота, керівника або виконавця, має потребу в контролі. **Контроль** як функція менеджменту дозволяє вчасно виявити «вузькі місця», невідповідність норм і нормативів дійсності, виправити їх або поправити дії працівників. У менеджменті вироблені найбільш загальні способи здійснення цих функцій. Вони названі **принципами менеджменту.**

Загальні принципи управлінської діяльності

У менеджменті **під принципами** розуміють слідування основним вихідним положенням теорії управління, внутрішні переконання менеджерів, що визначають їхнє відношення до своєї справи та норм поведінки в колективі. У своїй роботі менеджер керується не тільки принципами, але ще і конкретними способами досягнення поставлених цілей і рішення конкретних завдань. Ці способи або прийоми в управлінській діяльності називають **методами менедж-**

менту. Існує багато конкретних методів управлінської роботи, але основні з них два:

– заснований на позаекономічному примусі працівників до праці – **адміністративний метод;**

– заснований на економічному примусі до праці, за допомогою якого працівником рухає **економічний інтерес.**

Технократичний підхід до аналізу принципів управління дозволяє виділити три основні стадії розвитку промислового виробництва і відповідні їм принципи управління.

Перша стадія. Це початковий етап застосування машин у виробництві, на якому машинне виробництво будувалося виходячи з можливостей робітника, його фізичних даних, швидкості, умілості і інтенсивності праці, уміння управляти машиною. Тут людина була основою всього виробничого процесу. Однак кількісне збільшення машин поступово відсунув робітника на другі позиції, а на перше місце вийшла сама машина, техніка.

Друга стадія. Її називають промисловою. Роль робітника змінюється: він стає «частковим робітником», придатком машини. Управлінська робота будується за принципом технічного пріоритету. Виробництво оснащується необхідною технікою, розробляється технічна документація, створюється структура підприємств і його управління. Великі підприємства, використовуючи машинне виробництво, починають масове виробництво товарів, в результаті чого відбувається подальший внутрівиробничий поділ праці за функціональною ознакою. Техніка, технологія, постачання та збут продукції, забезпечення виробництва необхідними фахівцями почали здійснюватися за принципом від потреб машинного виробництва. Управління на цій стадії будується виходячи з можливостей техніки та технології. Основним принципом управління стає раціоналізація праці робітників: раціональна облаштованість робочого місця, відпрацьовування раціональних рухів працівників, пошук можливостей стимулювання більш інтенсивної праці. **Раціоналізм** став метою управління виробництвом, головним його принципом. Подальший розвиток продуктивних сил, обумовлений прогресом науки і техніки, призвів до значних змін у принципах управління, заснованих на раціоналізмі.

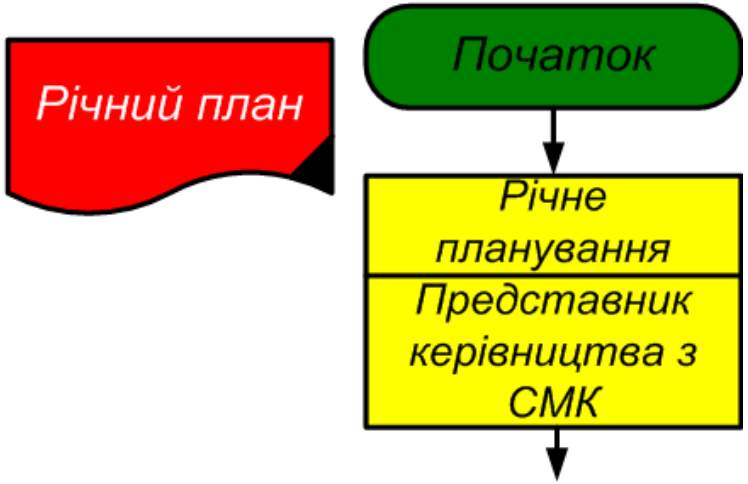


Рис. 5.3. Фрагмент вимог процедур з внутрішнього аудиту

Програма включає:

– всі елементи ISO 27001;

– підрозділи підприємства, в яких перевіряється даний елемент;

– прізвища призначених аудиторів;

– термін перевірки (місяць).

Інженер з ІБ знайомить призначених аудиторів з Програмою під підпис.

а) Керівництво підприємства може призначити позаплановий аудит у разі серйозних порушень в СМІБ.

б) Підрозділ, що підлягає аудиту, повідомляють про це не менш ніж за 24 години.

в) Якщо обсяг аудиту передбачає включення кількох людей, представник керівництва призначає старшого в цій групі.

г) Призначений аудитор несе відповідальність за планування, підготовку, проведення та складання звітності про виконання аудиту.

д) Підготовка до аудиту включає (див. рис. 5.4):

– вивчення процедури «Внутрішній аудит»;

– вивчення процедур по процесам, що перевіряються;

– складання Переліку контрольних питань.

Алгоритм проведення внутрішніх аудитів

0) Розробка процедури внутрішніх перевірок СМІБ:

а) підбір і навчання команди аудиторів;

б) розробка річного плану внутрішніх аудитів;

в) затвердження групи аудиторів і річного плану аудитів вищим керівництвом.

1) Розробка плану Конкретного аудиту:

а) визначення області (підрозділів);

б) визначення критеріїв (вимоги 27001, внутрішні правила, політики і процедури ІБ);

в) розробка анкетування (за критеріями, за підрозділами).

2) Проведення аудиту в підрозділах згідно з графіком;
3) Фіксування доказів аудиту;
4) Підготовка протоколу відхилень;
5) Розробка звіту про аудит;
6) Розробка коригувальних заходів;
7) Перевірка виконання коригувальних заходів;
8) Аналіз результативності коригувальних заходів.

Фрагмент вимог процедур з внутрішнього аудиту (див. рис. 5.3). Приклад

Представник керівництва з СМІБ відповідає за:

– планування аудитів з урахуванням важливості процесів, а також результатів попередніх аудитів;

– організацію проведення аудитів (Хто? Коли? ...);

– забезпечення звітності про аудити - основи для аналізу, оцінювання та вдосконалення процесів СМІБ.

До 10 січня поточного року інженер з ІБ розробляє Програму проведення внутрішніх аудитів на рік, керуючись при цьому:

– результатами минулих аудитів;

– важливістю процесів, що перевіряються;

– станом роботи підрозділів, планом проведення капітальних ремонтів в цехах;

– План погоджує представник керівництва з СМІБ і затверджує голова правління.

Аудит конкретного підрозділу проводиться не рідше 1 разу на рік.

Постіндустріальна стадія. На цій стадії розвитку продуктивних сил все більша увага керівників підприємств приділяється безпосередньо працівникові, фахівцеві, розкриттю його можливостей у підвищенні продуктивності праці. Перед управлінськими кадрами виникло інше завдання – не тільки забезпечити роботу підприємства новітньою технікою та технологіями, але і «вичавити» з них максимум можливого.

Як показала практика, досягти цього тільки за допомогою принципів раціоналізму неможливо. Необхідні нові принципи управління, які, не відкидаючи раціоналізму, а, удосконалюючи його, вели б до росту продуктивності праці. Таким загальним принципом управління став **принцип людських відносин.** Керівники змушені були звернути увагу на умови праці працівників, на зростання рівня їхньої потреб, зацікавленість їх у самому процесі праці, позбавити людей від монотонної, виснажливої, одноманітної та рутинної праці. Управління стало розвиватися у двох нових напрямках: по-перше, залучення на виробництво фахівців – соціологів і психологів; і, по-друге, пошук техніко-технологічних можливостей, здатних полегшити умови праці [2, 6]. Керуючись принципом людських відносин і раціоналізму, американські менеджери домоглися різкого підвищення продуктивності праці і інтенсивного використання нової техніки та технологій. По продуктивності суспільної праці в промисловості американці перевершували нас у два рази, а в сільському господарстві – у чотири рази.

У нашій країні, де панувала суспільна власність на засоби виробництва, головним визначальним принципом управління став **принцип планомірності.** Директивне планування стримувало можливість використовувати досягнення НТР у виробництві, а командно-адміністративна система управління виявилася недостатньо гнучкою для рішення завдань, які виникли. Проте, цілий ряд галузей промисловості, і особливо радіоелектронна промисловість, авіа- і приладобудування, оборонна промисловість, не тільки успішно працювали, але і були передовими у світі. Тут позначилося те, що принцип управління, заснований на планомірності при належній допомозі і матеріальній підтримці держави, державному контролі та належному стимулюванні праці працівників, дозволив кращим образом використати новації. Принцип планомірності лежить в основі першої функції менеджменту – планування. Він успішно

використовувався в самих різних умовах у нашій країні, а сьогодні широко застосовується всіма менеджерами світу.

У сучасних умовах становлення ринкової економіки у вітчизняній практиці управління необхідно взяти на озброєння все краще, що досягнуто західними вченими і практиками. Однак не слід керуватися таким підходом: «все, що в нас – погано, все що в них – добре»; сліпого копіювання принципів, придатних для американців, німців або японців, не повинно бути. Важливо враховувати, що західний менеджмент може стати корисним лише у випадку використання його стосовно до українських умов, звичок, традицій, особливостей поводження людей, рівню їхньої професійної підготовки, національним особливостям тощо.

1.2. Базові характеристики інформаційної безпеки

У тих випадках, коли йдеться про безпеку щодо інформації та інформаційно-обчислювальних систем, застосовуються загальноприйняті терміни про властивості цих об'єктів – категорії (див. рис. 1.1).

Рис. 1.1. Властивості ІБ

Інформація з точки зору інформаційної безпеки має наступні категорії:

– конфіденційність – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для якого вона призначена;

Контроль за станом здоров'я людини – це і є моніторинг системи/організму або самоконтроль.

– «Термометром» в різних підрозділах підприємства служить проведений аудит, що дозволяє встановити, чи виконуються заплановані задані показники.

Тому у даному розділі ми розглядаємо питання планування, проведення, оцінки та документування внутрішніх аудитів підприємства. Зазначені етапи аудитів роз'яснюються на прикладі внутрішнього аудиту системи.

Внутрішній аудит – це інструмент управління вищого керівництва. Метою проведення внутрішніх аудитів є перевірка того, що система менеджменту:

а) відповідає встановленим вимогам;

б) результативно впроваджена і підтримується в робочому стані.

Рекомендації з аудиту (ISO 19011).

Рекомендації з організації процесу аудиту містяться в ISO 19011 «Керівні вказівки з аудиту систем менеджменту» (див. рис. 5.2) [1].

Дані рекомендації застосовуються при проведенні перевірок СМЯ (ISO 9001), ІБ (ISO 27001) [2], професійної безпеки та охорони праці (на відповідність OHSAS 18001), систем управління безпечністю харчових продуктів (HACCP) і в морському судноплавстві (ISM Code), а також можуть бути застосовані при аудиті інших систем менеджменту.

Рис. 5.2. Алгоритм внутрішнього аудиту

– Як призначаються, плануються, готуються і проводяться внутрішні аудити системи?

– Хто на підприємстві проводить аудити і відповідає за це?

– Які результати приносять аудити, як вони документуються і сприяють процесу вдосконалення?

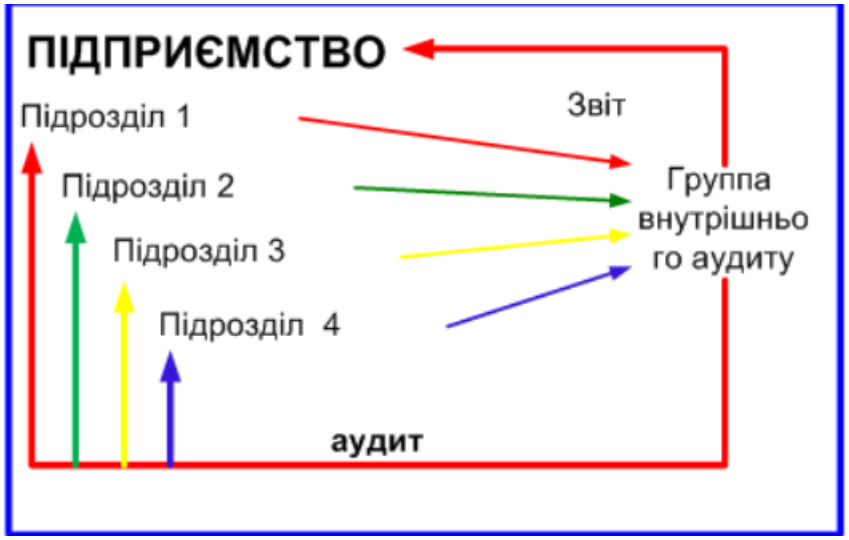


Рис. 5.1. Схема внутрішнього аудиту

Внутрішній аудит – це самоперевірка.

Чи це буде вимірювання температури і кров'яного тиску або тест на вміст цукру в крові – всі ми займаємося медичною самоперевіркою. Якщо, наприклад, наші показники температури, аналізи крові (фактичні значення) відхиляються від встановленого в медицині (заданого) значення 36,8°, необхідно з'ясувати причини підвищення температури і вжити відповідних заходів. Високу температуру часто можна пояснити вірусним грипом або застудою, і прийом відомих нам простих медикаментів (мікстур від кашлю, таблеток) і кілька днів постільного режиму виявляються достатніми для зниження температури. Але щоб попередити ці захворювання в майбутньому, можна зміцнювати імунну систему, наприклад, захисними щепленнями, заняттями спортом, відвідуваннями сауни і здоровим способом життя.

порушення цієї категорії називається розкраданням або розкриттям інформації;

– цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;

– автентичність – гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор, порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;

– апелювання – досить складна категорія, яка проте часто застосовується в електронній комерції – гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що, при підміні автора, хтось інший намагається заявити, що він автор повідомлення, а при порушенні апелювання – сам автор намагається «відхреститися» від своїх слів, підписаних ним одного разу.

Відносно інформаційних систем застосовуються інші категорії:

– надійність – гарантія того, що система в нормальному і позаштатному режимах поводиться так, як заплановано;

– точність – гарантія точного і повного виконання всіх команд;

– контроль доступу – гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;

– можливість контролю – гарантія того, що в будь-який момент може бути проведена повноцінна перевірка будь-якого компонента програмного комплексу;

– контроль ідентифікації – гарантія того, що клієнт, підключений в даний момент до системи, є саме тим, за кого себе видає;

– стійкість до навмисних збоїв – гарантія того, що при навмисному внесенні помилок в межах заздалегідь обговорених норм система буде поводитися так, як це було обумовлено заздалегідь.

Пояснимо поняття доступності, цілісності і конфіденційності.

Доступність – це можливість за прийнятний час отримати необхідну інформаційну послугу. Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованих змін. Нарешті, конфіденційність – це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (купуються) для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент ІБ.

Особливо яскраво провідна роль доступності проявляється в різного роду системах управління – управлінні виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги та ін.).

Цілісність можна поділити на статичну (незмінність інформаційних об'єктів) і динамічну (коректне виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність проявляє себе як найважливіший аспект ІБ в тих випадках, коли така інформація слугує «керівництвом до дії». Рецептура ліків, запропоновані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може виявитися в буквальному сенсі смертельним. Неприємним є і спотворення офіційної інформації, чи буде це текст закону, чи сторінка Web-сервера будь-якої урядової організації.

Конфіденційність – найбільш відпрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем стикається в Україні з серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, так що більшість користувачів не мають змоги отримати уявлення про

Розділ 5. АУДИТ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Внутрішній аудит

Внутрішній аудит СМІБ за вимогами ISO 27001 та ISO 19011

Організація повинна проводити внутрішній аудит СМІБ в заплановані терміни для визначення, чи відповідають цілі управління, засоби управління, процеси і процедури СМІБ наступним положенням:

а) відповідати вимогам даного Міжнародного стандарту і відповідним нормативним актам;

б) відповідати ідентифікованим вимогам ІБ;

в) ефективно забезпечуватися і підтримуватися;

г) працювати як очікується.

Програма аудиту повинна бути запланована з урахуванням розгляду статусу та важливості процесів і областей, схильних до аудиту, а також результатів попередніх перевірок.

Критерії аудиту, область діяльності, **періодичність та методи** проведення також повинні бути визначені.

Вибір аудиторів і проведення аудиту повинно забезпечувати **об’єктивність і неупередженість**. Аудитори не можуть здійснювати аудит своєї роботи.

Відповідальність і вимоги щодо планування та проведення аудитів, а також доповіді результатів і підтримок записів повинні бути визначені як **документована процедура**.

Відповідальність менеджменту за область, що піддається аудиту, повинна забезпечувати вживання заходів без надмірних затримок з метою усунення виявлених невідповідностей та їх причин.

Подальша діяльність повинна включати перевірку виконаних дій і доповідь результатів перевірки.

Зауваження: Керівництво по аудиту систем управління ISO 19011, може забезпечити корисне керівництво по проведенню внутрішніх аудитів СМІБ.

Аудит внутрішній (аудит першою стороною) – внутрішня перевірка (див. рис. 5.1).

Внутрішній аудит системи менеджменту

11) Автоматизированные информационные технологии в управлении финансовыми рисками коммерческого банка, [В. И. Соловьев, Е. В. Строганова и др.], М.: ПИК ВИНИТИ, 2005, с. 185.

12) Автоматизированная система типовых решений и анализа, Донецк: НИЦИТ ИЭП НАН Украины, 2004, с. 22.

13) Програмные Решения для Kayako. Модули для службы технической поддержки. Дополненный модуль “Assets”, Управление активами,[Электронный ресурс], Режим доступа: World Wide Web. – URL: http://kayako–solutions.ru/ dopolnennyiy–modul –assets– upravlenie– aktivami/

14) IBM. Systems. Asset management., [Electronic Resource], Mode of access: URL:http://publib.boulder.ibm.com/ infocenter/tivihelp/ v27r1/ index.jsp?topic=%2 Fcom.ibm.itam.doc%2 Foverview%2Ftamit_ovr_c_assetma.

15) Управление активами и оптимизация активов [Электронный ресурс], Режим доступа: URL: http://www.flowserve.com/ files/ Files/ Literature/ ProductLiterature/ Pumps/fsg–104–r.pdf.

16) **А. Романюк,** IBM Maximo – полный цикл управления активами предприятия, [Электронный ресурс], Режим доступа: URL: http://sibis.com.ua/ contents/ article/ index/ section/ 329/article/677.

17) АБК Оценка [Электронный ресурс]: Оценка активов предприятия, Режим доступа: World Wide Web. – URL: http://xn—80aacqybug6e. xn—p1ai/?servpage=72.

18) У. Бернстайн, Разумное распределение активов, Изд.: «Лори», 2005.

потенційні ризики. По-друге, на шляху користувацької криптографії як основного засобу забезпечення конфіденційності постають численні законодавчі перепони і технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує інформаційну систему (ІС), на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить перекручені дані?

Нарешті, конфіденційні моменти також присутні у багатьох організаціях (навіть в згадуваних вище навчальних інститутах намагаються не розголошувати відомості про зарплату співробітників) і окремих користувачів (наприклад, паролі).

Приклади порушення КОНФІДЕНЦІЙНОСТІ:

– потрапляння комерційної інформації до конкурентів або до неавторизованої сторони (НАС);

– доступ третіх осіб до інформації, що містить комерційну таємницю.

Приклади порушення ДОСТУПНОСТІ:

– несвоєчасність отримання інформації, необхідної для отримання послуги клієнтом банку;

– зупинка робочого процесу підрозділів, робота яких вимагає постійної наявності телефону / факсу.

Приклади порушення ЦІЛІСТНОСТІ:

– некоректність отриманої інформації для виконання оперативних бізнес-цілей;

– неточність даних про одержувача кредиту.

Поширені помилкові судження про ІБ:

«У нас ніколи не було жодних інцидентів, пов’язаних з інформацією»

Така думка, швидше за все, базується на тому, що інциденти, пов'язані з інформацією, не фіксуються, а постійно і «тихо» усуваються на місцях. При цьому має місце приховування, що тягне за собою додаткові витрати, про які керівництву нічого не відомо.

«Нікому не потрібна наша інформація, вона не є таємницею»

У пресі все частіше з'являються повідомлення про рейдерські напади, про катастрофу надійних міжнародних брендів в зв'язку з компрометацією, про зупинку виробництва через діяльність третіх осіб. Цей підхід ілюструє нерозуміння всієї широти менеджменту інформаційної безпеки. Питання конфіденційності – це тільки одне з трьох основних питань безпеки. Ще існує два, часто навіть важливіші, аспекти: доступність інформації та її цілісність.

«Наші мережі, програмне та комп'ютерне забезпечення надійно захищені»

Це твердження часто ґрунтується на тому, що менеджмент витрачає чималі кошти на технічні засоби. Але чи може менеджмент бути впевненим у тому, що ці кошти витрачені правильно, тобто з максимальною вигодою для підприємства? Потрібно чітко розрізняти всі небезпеки (не тільки комп'ютерні), оцінювати їх і слідкувати, щоб процес забезпечення безпеки працював постійно.

«Ми довіряємо нашим співробітникам і впевнені в тому, що вони виконують всі вимоги з безпеки»

Статистика говорить про те, що найбільша частина інцидентів в ІБ відбувається з безпосередньої вини співробітників. Необхідні дії по забезпеченню ІБ при прийомі на роботу співробітників, в процесі виконання службових обов'язків, при переході на іншу посаду, при звільненні.

Визнаний підхід до ІБ

Безпека – це НЕ продукт:

– Безпеку не можна купити, безпеку потрібно створювати!

– При створенні безпеки слід спиратися на вже існуючі продукти (ресурси).

Безпека – це НЕ проект:

– Недостатньо створити безпеку один раз, безпеку потрібно підтримувати постійно!

– Створення та підтримку безпеки можна здійснювати у вигляді проектів.

→ **Безпека – це процес** [7].

СПИСОК ЛІТЕРАТУРИ ДО ЧЕТВЕРТОГО РОЗДІЛУ

1) «Методи захисту системи управління інформаційною безпекою», Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП «УкрНДНЦ», 2016, с. 28.

2) «Information technology. Security techniques. Code of practice for information security controls», ISO/IEC 27002:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 80.

3) «Information technology. Security techniques. Information security management systems implementation guidance», ISO/IEC 27003:2017, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017, p. 45.

4) В.В. Кириленко, Економіка (навчальний посібник) [Електронний ресурс], Тернопіль: Економічна думка, 2002, с. 193, Режим доступу: World Wide Web. – URL: http://buklib.net/books/26834/

5) Asset management, Overview, principles and terminology (ISO 55000:2014) [Electronic Resource], Mode of access: URL: http:// www.iso.org/ iso/ru/ catalogue_detail?csnumber=55088.

6) Управление активами. Элементы системы управления активами: семинар Стандарты ISO серии 55000 НПП «СпецТек» [Электронный ресурс], Режим доступа: World Wide Web. – URL: http://www. trim.ru/ content/view/697/211/

7) В.И. Иорш, И.Э. Крюков, И.Н. Антоненко, Международные стандарты в области управления физическими активами [Электронный ресурс], Режим доступа: URL: http://www.trim.ru /docs/ Asset_management_standard.pdf.pdf

8) Publicly Available Specification for the optimal management of physical assets (PAS 55:2008) [Electronic Resource], Mode of access: World Wide Web. – URL: http://www.assetmanagementstandards.com/ PAS55.html

9) SAE standards [Electronic Resource], Mode of access: World Wide Web., URL: http://standards.sae.org.

10) И.А. Бланк, Управление активами и капиталом предприятия, К.: Ника – Центр, Эльга, 2003.

8) Що включає в себе управління доступом?

9) Яке криптографічне забезпечення необхідно впроваджувати під час побудови СМІБ?

10) Що входить до системи фізичної безпеки підприємства?

11) Як забезпечується безпека виробничих процесів організації?

12) Які процедури забезпечують безпеку комунікацій?

13) Які етапи впровадження та експлуатації ІС?

14) Як забезпечується ІБ у відносинах з постачальниками?

15) Що включає в себе управління інцидентами ІБ?

16) ЯК забезпечується неперервність бізнесу з точки зору ІБ?

1.3. Базові поняття системи менеджменту інформаційної безпеки

Актив (asset) – що-небудь, що представляє цінність для організації.

Аналіз ризику (risk analysis) – систематичне використання інформації для виявлення джерел і для оцінки ступеня ризику.

Аналітична модель (analytical model) – алгоритм або розрахунок, що включає одну або більше основних мір і / або похідних заходів (похідних мір), з відповідним критеріями прийняття рішень.

Атака (attack) – спроба знищити, розкрити, змінити, зробити недоступним, вкрасти або отримати несанкціонованиӣ доступ або несанкціоновано використовувати актив.

Атрибут (attribute) – властивість або характеристика об'єкта, відмінність якого (кількісне або якісне) від іншого може бути встановлено безпосередньо людиною або автоматизованими засобами.

Аудит (audit) – систематичниӣ, незалежниӣ і задокументованиӣ процес отримання свідоцтва аудиту та об’єктивної його оцінки з метою визначення ступеня, з яким виконуються критерії аудиту.

Автентифікація (authentication) – забезпечення гарантії того, що заявлені характеристики об'єкта є справжніми.

Безперервність ІБ (information security continuity) – *процеси* і процедури, що гарантують постійне забезпечення ІБ.

Верифікація (verification) – підтвердження отриманням об'єктивних свідчень, що задані вимоги були виконані.

Вище виконавче керівництво (executive management) – особа або група осіб, кому делеговано *керівним органом управління* відповідальність за реалізацію стратегії і політик для досягнення цілей *організації.*

Уразливість (vulnerability) – слабке місце активу або *засобів управління*, яке може бути використано однією або більше *загрозами*.

Достовірність (authenticity) – властивість, що вказує, що об'єкт являє собою те, що він заявляє про себе.

Доступність (availability) – властивість інформації бути доступною і придатною до використання на вимогу уповноваженої особи.

Загроза (threat) – можлива причина небажаного інциденту, який може завдати шкоди системі або організації.

Залишковий ризик (residual risk) – ризик, що залишається після обробки ризику.

Захист інформації (information security) – збереження конфіденційності, цілісності та доступності інформації; крім того, також можуть бути включені інші властивості, такі як автентичність, підзвітність, апелювання і надійність.

Інформаційна система (information system) – додатки, служби, активи, пов'язані з ІТ, або інші компоненти обробки інформації.

Інцидент в системі захисту інформації (information security incident) – одна або серія небажаних або несподіваних подій в системі захисту інформації (СЗІ), які мають великий шанс скомпрометувати ділові операції і поставити під загрозу захист інформації (ЗІ).

Інцидент ІБ (information security incident) – одне або кілька небажаних або несподіваних *подій ІБ*, які зі значним ступенем вірогідності наражають на небезпеку ділову діяльність і загрожують ІБ.

Компетентність (competence) – здатність застосовувати знання та навички для досягнення бажаних результатів.

Конфіденційність (confidentiality) – властивість, що інформація не буде доступною або розголошеною не уповноваженим особам, організаціям або процесам.

Критерій прийняття рішення (decision criteria) – порогові, цільові або еталонні значення, використовувані для визначення необхідності дії або подальшого аналізу, або для опису рівня впевненості в даному результаті.

Критерій ризику (risk criteria) – еталонні умови, на підставі яких оцінюють значимість *ризику.*

Менеджмент інцидентів інформаційної безпеки (information security incident management) – *процеси* виявлення, інформування, оцінки, реагування, обробки і винесення уроків з *інцидентів ІБ.*

Менеджмент ризиків (risk management) – узгоджені види діяльності з керівництва та управління організацією щодо ризиків.

Можливість застосування (availability) – властивість доступності і готовності до використання за авторизованим запитом.

Технічна відповідність повинна аналізуватися переважно за допомогою автоматизованих інструментів, які генерують звіти для подальшої їх інтерпретації технічним фахівцем. Крім цього, аналіз може виконуватися вручну (з використанням відповідних програмних засобів, якщо необхідно) досвідченим системним інженером.

Якщо застосовуються тести на проникнення або оцінки уразливостей, то необхідно робити попередження, так як така активність може вести до порушення безпеки системи. Такі тести повинні плануватися, документуватися і повторюватися. Будь-який аналіз технічної відповідності повинен виконуватися тільки компетентними і авторизованими особами або під керуванням таких осіб.

Аналіз технічної відповідності включає перевірку діючих систем, щоб гарантувати, що засоби управління обладнанням і ПЗ здійснюються належним чином. Даний тип аналізу відповідності вимагає фахівця з технічної експертизи.

Аналіз відповідності також включає в себе, наприклад, тест на проникнення і оцінку уразливостей, які можуть виконуватися незалежними експертами, запрошеними для цих цілей. Це може бути корисним при визначенні уразливостей в системі та для перевірки, наскільки результативні засоби управління в попередженні несанкціонованого доступу з використанням цих уразливостей.

Тест на проникнення і оцінка уразливостей дає миттєвий знімок системи в конкретному стані на конкретний момент часу. Це уявлення обмежена тією частиною системи, яка піддавалася тестуванню при спробах проникнення. Тест на проникнення і оцінка уразливостей не замінюють собою оцінки ризиків. Стандарт ISO / IEC 27008 дає конкретні рекомендації, пов'язані з аналізом технічної відповідності [1, 2].

Питання для самоконтролю

1) Що таке політика ІБ?
2) Які політики можуть входити до загальної політики СМІБ?
3) З чого складається організаційне забезпечення ІБ?
4) Які етапи включає у себе забезпечення безпеки персоналу?
5) В які кроки реалізується управління активами?
6) Які існують стандарти забезпечення управління активами?
7) Які існують програмні засоби підтримки управління активами?

єю, що спеціалізується на подібного роду оцінках. Ті, хто проводить такі перевірки, повинен володіти відповідними навичками та досвідом.

Результати незалежного аналізу повинні бути зафіксовані і передані керівництву, яке ініціювало аналіз. Ці записи повинні зберігатися.

Якщо незалежний аналіз виявляє неадекватність підходу до управління ІБ та його реалізації в організації, наприклад, документовані завдання і вимоги не виконуються або не узгоджуються з положеннями, сформульованими в політиках ІБ, керівництво повинно розглянути необхідність коригувальних дій.

Стандарти ISO / IEC 27007 «Керівництво з аудиту СМІБ» і ISO / IEC TR 27008 «Керівництво для аудиторів з перевірки засобів менеджменту ІБ» також дають рекомендації з проведення незалежного аналізу.

2) Відповідність політикам і стандартам безпеки. Керівники повинні регулярно перевіряти відповідність оброблення інформації та процедур у межах сфери їх відповідальності належним політикам, стандартам та іншим вимогам щодо безпеки.

Керівники повинні визначити, яким чином аналізувати виконання вимог ІБ, визначених у політиках, стандартах та інших чинних нормах. Необхідно розглянути можливість застосування інструментів автоматизованого вимірювання та формування звітів для забезпечення ефективного регулярного аналізу.

У разі виявлення в результаті аналізу будь-якої невідповідності, керівники повинні:

а) визначити причини невідповідності;

б) оцінити необхідність дій для забезпечення відповідності;

в) виконати відповідні коригувальні дії;

г) оцінити результативність коригувальних дій і виявити будь-які недоліки і слабкості.

Результати аналізу та коригуючих дій, здійснених керівниками, повинні бути зафіксовані і ці записи повинні зберігатися. Керівники повинні передавати ці результати особам, які виконують незалежний аналіз, коли такий аналіз проводиться в сфері їх відповідальності.

3) Перевірка технічної відповідності. ІС потрібно регулярно перевіряти на відповідність політикам і стандартам ІБ організації.

Моніторинг (monitoring) – визначення стану системи, *процесу* або роботи.

Невідповідність (nonconformity) – невиконання *вимоги.*

Обробка ризику (risk treatment) – процес вибору і реалізації заходів щодо зміни ризику.

Основна міра (base measure) – *міра*, встановлена відносно *атрибута* і методу його кількісного оцінювання.

Оцінка значущості ризику (risk evaluation) – процес порівняння розрахункового ризику із заданими критеріями ризику, з метою визначити значущість ризику.

Оцінка ризику (risk assessment) – цілісний процес аналізу ризику та оцінки значущості ризику.

Подія в СЗІ (information security event) – виявлений випадок системи, послуги або стану мережі, що вказує на можливе порушення політики захисту інформації або порушення в роботі засобів захисту, або невідома раніше ситуація, яка може мати значення для захисту.

Подія ІБ (information security event) – встановлене виникнення стану системи, служби або мережі, що вказує на можливе порушення політик ІБ або недостатність засобів управління, або на раніше невідому ситуацію, яка може бути істотною з точки зору безпеки.

Політика (policy) – наміри і напрямок розвитку *організації*, офіційно сформульовані вищим *керівництвом.*

Прийняття ризику (risk acceptance) – обґрунтоване рішення прийняти конкретний ризик.

Проект СМІБ (ISMS project) – структуровані дії, що впроваджуються організацією для впровадження системи управління ІБ.

Процес менеджменту ризику (risk management process) – систематичне застосування політик, процедур і встановлених методик до дій з обміну інформацією, консультацій, встановлення контексту, а також ідентифікації, аналізу, визначення ступеня, обробці, моніторингу та повторного аналізу *ризику.*

Система менеджменту (management system) – сукупність взаємопов'язаних або взаємодіючих елементів *організації* для розробки *політик* і *цілей*, а також *процесів* для досягнення цих цілей.

Система менеджменту інформаційної безпеки (information security management system) (ISMS) – частина загальної системи

менеджменту, заснованої на управлінні ризиками, для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані й покращення ЗІ.

Управління доступом (access control) – механізми, покликані гарантувати, що доступ до активів дозволений і обмежується відповідно до вимог бізнесу і безпеки.

Управління інформаційною безпекою (governance of information security) – система, за допомогою якої спрямовуються і контролюються дії *організації* у сфері ІБ.

Цілісність (integrity) – властивість збереження точності і повноти активів [8, 9].

Активи (ресурс) – основні об'єкти ІБ.

Інформаційний актив (ресурс) – матеріальний чи нематеріальний об'єкт, який:

- є інформацією або містить інформацію;
- має цінність для організації.

Прості активи (ресурси):

- законодавча база;
- рекламні пропозиції;
- фінансові звіти тощо.

Складні активи (ресурси):

- сервер підприємства;
- ноутбук керівника підприємства та ін.

1.4. Місце і види інформації

Інформація на підприємстві – аналог центральної нервової системи організму людини.

За допомогою інформації:

- приймаються управлінські рішення;
- віддаються команди на виконання тих чи інших бізнес-операцій (див. рис. 1.2);
- здійснюється накопичення знань (навичок);
- здійснюється взаємодія структурних підрозділів.

У кінцевому підсумку інформація служить обов'язковим провідником для виконання поставлених цілей за якістю, кількістю, вартістю випуску продукту або послуги.

персональну інформацію, а також можуть обмежувати можливість передачі персональної інформації в інші країни.

5) Нормативи щодо криптографічних засобів. Криптографічні засоби потрібно використовувати відповідно до всіх застосовних угод, законів та регуляторних вимог.

Для відповідності з чинними угодами, законодавчими та нормативними актами необхідно врахувати наступне:

а) обмеження на імпорт і експорт комп'ютерної техніки та ПЗ, що здійснює криптографічні функції;

б) обмеження на імпорт і експорт комп'ютерної техніки та ПЗ, які розроблені з можливістю додавання в них криптографічних функцій;

в) обмеження на застосування шифрування;

г) примусово чи добровільно застосовуються методи доступу органів державної влади до інформації, зашифрованою пристроями або ПЗ для захисту конфіденційності змісту.

Необхідно заручитися юридичною підтримкою, щоб гарантувати відповідність з чинними угодами, законодавчим та нормативним актам. До того, як зашифрована інформація або криптографічні засоби будуть переміщені з однієї юрисдикції в іншу, повинні бути отримані юридичні рекомендації.

Перевірки ІБ

Ціль: гарантувати, що ІБ впроваджена та працює відповідно до організаційних політик та процедур.

1) Незалежні перевірки ІБ. Підходи організації до управління ІБ та її впровадження (тобто цілі заходів безпеки, заходи безпеки, політики, процеси й процедури для ІБ) мають незалежно перевірятися через заплановані інтервали або коли відбуваються значні зміни.

Керівництво повинно ініціювати проведення незалежного аналізу. Такого роду незалежний аналіз необхідний, щоб гарантувати постійну придатність, адекватність і результативність підходу організації до управління ІБ. Аналіз повинен включати в себе оцінку можливостей для покращення та необхідності змін в підході до безпеки, в тому числі політики та завданнях управління.

Такий аналіз повинен проводитися людьми, не пов'язаними з аналізованою областю, наприклад, тими, хто проводить внутрішні аудити, керівниками інших напрямків або зовнішньою організаці-

працює в межах, встановлених законом, або нормативних правил, щоб забезпечити захист від можливого переслідування в рамках цивільного або кримінального права, або щоб підтвердити фінансовий статус організації її зацікавленим особам, зовнішнім сторонам і аудиторам. Національне законодавство або норми можуть встановлювати період зберігання і утримання для інформації, що зберігається.

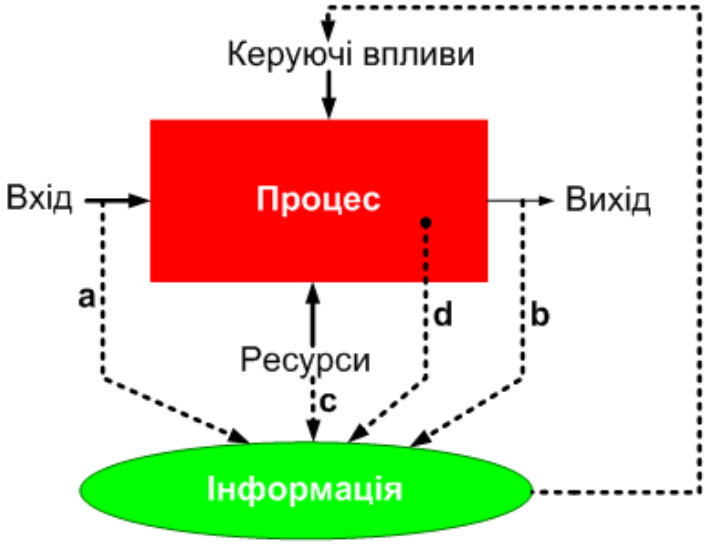
Додаткова інформація про управління записами організації може бути знайдена в ISO 15489-1.

4) Захист даних та конфіденційність персональних даних. Конфіденційність і захист даних, що ідентифікують особу, має бути забезпечено згідно з вимогами відповідного законодавства та регуляторними вимогами, за наявності.

Повинна бути розроблена і впроваджена політика організації щодо конфіденційності та захисту персональних даних. Ця політика повинна бути доведена до всіх, хто бере участь в обробці персональних даних. Дотримання цієї політики і всім відповідним законодавчим актам і нормам, пов'язаним із захистом приватного життя людей і персональних даних, вимагає відповідної управлінської структури і контролю.

Часто це найкращим чином досягається призначенням відповідальної особи, наприклад, відповідального за охорону особистої інформації, який повинен розробити інструкцію для керівників, користувачів і постачальників послуг, визначальну їх персональні обов'язки і конкретні процедури, яких необхідно дотримуватися. Призначення відповідальності за обробку персональних даних та забезпечення знання принципів збереження конфіденційності повинні бути здійснені відповідно до чинного законодавства і норм. Повинні бути виконані відповідні технічні та організаційні заходи щодо захисту персональної інформації.

Стандарт ISO 29100 представляє високорівневу концепцію захисту персональної інформації в застосуванні до систем інформаційно-комунікаційних технологій. Чимало країн уже ввели законодавчі акти, що встановлюють механізми збору, обробки і передачі персональних даних (зазвичай це інформація про живих людях, які можуть бути ідентифіковані на підставі цієї інформації). Залежно від відповідного національного законодавства такі механізми можуть накладати обов'язки на тих, хто збирає, обробляє і розсилає



Інформація про Вхід – *a*;
Інформація про Вихід – *b*;
Інформація про Ресурси – *c*;
Інформація про Будову процесу – *d*;
Керуючі впливи = *F(a, b, c, d)*.

Рис. 1.2. Схема бізнес-процесу

Керуючі впливи – це функція від чотирьох змінних *a, b, c* і *d* (див. рис. 1.3).

Інформація утворює інформаційні потоки, які часто формуються на папері або в усному мовленні, потім перетворюються в електронний документ, пересилаються за допомогою електронної пошти (факсу), а потім можуть бути роздруковані на папері.

Інформація, необхідна для прийняття управлінських рішень:

а) економічні показники роботи власного підприємства і підприємств-конкурентів (товарообіг, прибуток та ін.);

б) дані про функціонування бізнес-процесів підприємства (схеми бізнес-процесів, збої в роботі процесів, можливості поліпшення бізнес-процесів);

в) дані про роботу постачальників (якість поставок, наявність альтернативних постачальників);

г) дані про ринок збуту (потреби і рівень задоволення клієнтів).

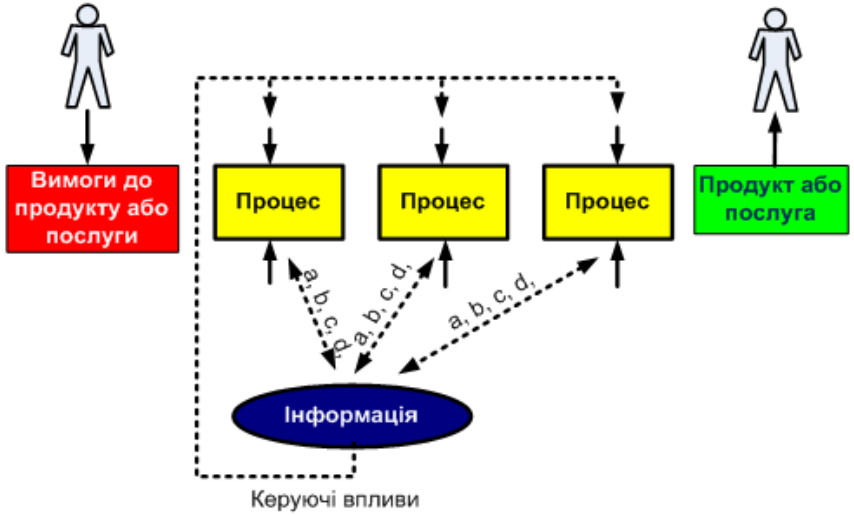


Рис. 1.3. Загальна схема використання інформації

Інформація, необхідна для виконання оперативних бізнес-цілей:

а) результати управлінських рішень (адміністративні накази, інновації);

б) оперативні завдання і коригування (оперативні плани, коригування планів);

в) інформація про сировину і матеріали (залишки на складі, терміни поставок, якість сировини);

г) вимоги замовників (контракти, побажання).

Інформація, необхідна для забезпечення (роботи) бізнес-процесів і роботи підприємства в цілому:

а) опис процесів і їх взаємозв'язку (стандарти підприємства, процедури, оргструктура);

б) методична документація (інструкції, довідкові посібники);

в) адміністративна документація (посадові інструкції, внутрішні правила, накази).

Інформаційні уразливості – приклад.

Некоректність отримання інформації для виконання оперативних бізнес-цілей:

засновану на схемі класифікації організації. Записи повинні бути розподілені за категоріями різних типів, наприклад, облікові записи, бази даних, журнали транзакцій, контрольні журнали і операційні процедури, кожен зі своїм терміном зберігання і типом допустимого носія для зберігання, наприклад, папір, мікрофіши, магнітні та оптичні носії. Будь-які пов'язані криптографічні ключі та програми, пов'язані з зашифрованими архівами, або цифрові підписи повинні також зберігатися протягом терміну зберігання з можливістю дешифрування записів.

Повинна бути врахована можливість погіршення якості носія, використовуваного для зберігання записів.

Процедури зберігання і обробки повинні виконуватися відповідно до рекомендацій виробника.

У тих випадках, коли вже обраний електронний носій, повинні бути розроблені процедури, які б могли гарантувати можливість доступу до даних (як у фізичному сенсі, так і в частині читання формату) протягом всього терміну зберігання із захистом від втрати при технологічній зміні в майбутньому.

Системи зберігання даних повинні бути обрані так, щоб необхідні дані могли бути отримані в прийнятний час і прийнятному форматі, в залежності від вимог, які повинні бути виконані.

Система зберігання та обробки повинна гарантувати ідентифікацію записів та їх строків зберігання, як це визначено національним або регіональним законодавством або нормами, якщо це може бути застосовано. Ця система повинна допускати відповідну ліквідацію записі після закінчення терміну зберігання, якщо вони більше не потрібні організації. Щоб виконати ці завдання щодо захисту записів, в організації повинні бути зроблені наступні кроки:

а) повинні бути розроблені керівництва за термінами зберігання, процедури зберігання, обробки і ліквідації записів та інформації;

б) повинен бути розроблений порядок зберігання із зазначенням записів і їх термінів зберігання;

в) повинен зберігатися реєстр джерел ключової інформації.

Деякі записи можуть вимагати захищеного зберігання для виконання законодавчих, нормативних або контрактних вимог, а також для забезпечення суттєво важливої бізнес-діяльності. Прикладом є записи, які можуть вимагатися, як свідчення того, що організація

е) виконання засобів управління, щоб гарантувати, що максимально дозволена, ліцензією, кількість користувачів не перевищено;

ж) проведення перевірок на предмет того, що встановлено тільки авторизоване ПЗ та ліцензійні продукти;

з) розробка політики для забезпечення виконання умов ліцензій;

и) розробка політики для утилізації або передачі ПЗ іншим;

к) відповідність умовам і обмеженням для ПЗ та інформації, отриманих з мереж загального користування;

л) не копіювати, не конвертувати в інший формат і не витягувати з комерційних медіа-продуктів (фільм, аудіо запис) нічого, крім того, що дозволено законом про авторські права;

м) не копіювати повністю або частково книги, статті, звітні матеріали або інші документи, крім того, що дозволено законом про авторські права.

Права на інтелектуальну власність включають в себе авторські права на ПЗ або документи, права розробника, торгові марки, патенти і ліцензії на вихідний код. Програмні продукти, захищені авторським правом, поставляються зазвичай з ліцензійною угодою, яка визначає положення і умови ліцензії, наприклад, обмеження використання продуктів тільки конкретними пристроями або обмеження копіювання тільки створенням резервних копій. Важливість і усвідомлення прав інтелектуальної власності на ПЗ, що розробляється в організації, повинні бути доведені до персоналу.

Законодавчі, нормативні та контрактні вимоги можуть встановлювати обмеження на копіювання матеріалів, захищених авторським правом. Зокрема, вони можуть вимагати, щоб використовувалися тільки матеріали, розроблені організацією, або ліцензовані, або отримані організацією від розробника. Порушення авторського права може вести до юридичних наслідків, які можуть передбачати штрафи та кримінальне переслідування.

3) Захист організаційних записів. Відповідно до законодавчих, регуляторних, контрактних і бізнес-вимог важливі записи має бути захищено від втрати, знищення, фальсифікації, несанкціонованого доступу та несанкціонованого використання.

При вирішенні питань, пов'язаних із захистом конкретних записів організації, необхідно розглянути їх відповідну класифікацію,

а) помилки оператора через недостатню кваліфікацію або недостатній рівень контролю введення даних;

б) помилки в розрахунках через неуважність планувальників;

в) некоректна інтерпретація відділом маркетингу вимог замовника.

Зупинка робочого процесу підрозділів, робота яких вимагає постійної наявності телефону/факсу, локальної або глобальної мережі, вихід з ладу центрального сервера:

а) пошкодження комунікацій внаслідок проведення будівельно-ремонтних робіт;

б) несвоєчасна оплата послуг зв'язку;

в) збій в роботі серверного або клієнтського програмного забезпечення.

Використання старих версій адміністративних документів, відсутність чіткої ідентифікації версії документа:

а) наявність старих версій документів в місцях їх застосування;

б) використання неврахованих копій документів [7].

1.5. Цикл PDCA

У стандарті ISO 27001 описана загальна модель СМІБ, в основу якої покладено процесний підхід, для чого продемонстровано циклічний характер функціонування системи взаємопов’язаних метапроцесів (самостійних видів діяльності), регламентованих цим стандартом [8]. Крім того, стандартом зазначається, що до всіх процесів СМІБ можна застосовувати методологію, відому як цикл «PIan-Do-Check-Act» (PDCA) («Плануй-Виконуй-Перевіряй-Дій») [8, 10]. Цикл PDCA у стандартах ISO серії 27000 описується як сукупність послідовно виконуваних фаз у межах кожного виду діяльності, що обумовлює можливість управління цією діяльністю через зворотній зв’язок. Також підкреслюється можливість застосування методології PDCA як в межах окремих процесів різного масштабу, так і на рівні всієї організації загалом. При цьому у самому стандарті ISO 27001 наведені фази циклу PDCA відносно всієї СМІБ організації, описані таким чином [8, 10]:

Плануй: встановлюй цілі та процеси ІБ, потрібні для отримання результатів, що відповідають вимогам замовника та політиці організації.

Виконуй: упроваджуй процеси ІБ.

Перевіряй: відстежуй і вимірюй процеси ІБ, зважаючи на політику, цілі та вимоги до ІБ, а також звітуй про результати.

Дій: вживай заходів для постійного покращення показників функціонування процесів ІБ.

Водночас у багатьох інших стандартах ISO наочно демонструється можливість імплементації циклу PDCA при реалізації тих чи інших окремих видів діяльності. Прикладами таких стандартів можуть бути: ISO 10015 (управління циклом навчання персоналу); ISO 10012 (система керування вимірюваннями); ISO 10002 (система розглядання скарг); ISO 10013 (система управління документообігом); ISO 19011 (управління програмою аудитів) тощо.

Відомо, що цикл, згодом названий Циклом Демінга-Шухарта, вперше був запропонований американським вченим У. Шухартом (Walter A. Shewhart) ще у 1939 р., коли ним була обґрунтована необхідність статистичного управління процесами виробництва з метою забезпечення й постійного підвищення їх стабільності. У. А. Шухарт довів необхідність реалізації триступеневого циклу, що включав розробку специфікацій (вимог) на кожен вид продукції із зазначенням розрахованих допусків по кожному показнику якості, виготування продукції із дотриманням визначених умов, а також вибірковий контроль усіх специфікованих показників [10]. Результати контролю Уолтер Шухарт пропонував використовувати на кожному наступному циклі для внесення змін у специфікації та для коригування процесів виробництва. Така концепція передбачає внесення будь-яких змін у виробничі процеси виключно на основі результатів адекватного статистичного аналізу даних, одержуваних шляхом зворотного зв'язку.

Згодом цей підхід трансформувався в один з принципів сучасного менеджменту якості – «Прийняття рішень на основі фактів», який і було покладено в основу стандартів ISO серії 9000, починаючи з версії 2000 р. Едвардс Демінг (W. Edwards Deming), послідовник Шухарта, на початку 1950-х рр. запропонував традиційній цикл Шухарта розглядати як чотирьохфазну послідовність дій: планування процесу, виконання запланованого, всебічна оцінка результатів, а також дії, вживані для удосконалення процесу (рис. 1.4) [10].

4.14. Відповідність нормативно-правовому забезпеченню

Відповідність правовим та контрактним вимогам

Ціль: уникнути порушень будь-якого закону, вимог, що діють на підставі закону, нормативних або контрактних зобов'язань, пов'язаних з ІБ та будь-якими вимогами щодо безпеки.

1) Ідентифікація застосовного законодавства та контрактних вимог. Усі важливі вимоги, що діють на підставі закону, нормативні чи контрактні вимоги та підхід організації до задоволення цих вимог має бути чітко визначено, задокументовано та актуалізовано для кожної ІС та організації.

Конкретні засоби управління і персональні зобов'язання повинні бути визначені і документовані. Керівники повинні визначити всі законодавчі акти, що діють в їх організації, для того, щоб виконувати вимоги, які пред'являються для даного виду бізнесу. Якщо організація веде бізнес в інших країнах, керівники повинні мати на увазі виконання вимог у всіх відповідних країнах.

2) Права інтелектуальної власності. Має бути впроваджено належні процедури забезпечення відповідності законодавчим, нормативним і контрактним вимогам щодо прав інтелектуальної власності та щодо використання запатентованих продуктів ПЗ.

Для захисту будь-якого матеріалу, який може розглядатися як інтелектуальна власність, необхідно взяти до уваги такі рекомендації:

а) оприлюднення політики в сфері дотримання прав інтелектуальної власності, яка визначає законне застосування ПЗ та інформаційних продуктів;

б) отримання ПЗ тільки з відомих і надійних джерел, щоб гарантувати, що авторські права не порушені;

в) забезпечення обізнаності про політики щодо захисту прав інтелектуальної власності та попередження про рішучість вживаних заходів дисциплінарного впливу до тих, хто порушує їх;

г) підтримка в актуальному стані відповідних реєстрів активів і виявлення всіх активів, щодо яких діє вимога захисту прав інтелектуальної власності;

д) збереження доказів і свідчень володіння ліцензіями, майстер-дисками, посібниками і т.д.;

Організації повинні перевіряти безперервність управління ІБ за допомогою:

а) випробування і тестування функціональності процесів, процедур і засобів управління безперервністю ІБ, щоб гарантувати, що вони відповідають цілям забезпечення безперервності ІБ;

б) випробування і тестування даних і порядку виконання процесів, процедур і засобів управління безперервністю ІБ, щоб гарантувати, що результати їх здійснення відповідають цілям забезпечення безперервності ІБ;

в) аналізу придатності та результативності заходів забезпечення безперервності ІБ при зміні ІС, процесів забезпечення ІБ, процедур і засобів управління або процесів управління безперервністю бізнесу/відновленням після надзвичайних ситуацій, а також застосовуваних рішень.

Перевірка засобів управління безперервністю ІБ відрізняється від загальної перевірки ІБ і повинна виконуватися поза рамками тестування змін. Якщо можливо, краще об'єднати перевірку засобів управління безперервністю ІБ з тестами забезпечення організацією безперервності бізнесу або відновлення після надзвичайних ситуацій.

Резервне обладнання

Ціль: гарантувати доступність обладнання для оброблення інформації.

Доступність обладнання для оброблення інформації. Обладнання оброблення інформації має бути впроваджено з резервуванням, достатнім для того, щоб відповідати вимогам доступності.

Організація повинна визначити бізнес-вимоги до можливості застосування ІС. Там, де можливість застосування не може бути гарантована використанням існуючої системної архітектури, повинен бути розглянутий варіант резервування.

Де це може бути застосовано, резервні ІС повинні бути перевірені, щоб гарантувати, що перехід з одного компонента на інший працює, як заплановано.

Введення надмірності може призводити до ризиків для цілісності або конфіденційності інформації та ІС, які необхідно враховувати при проектуванні ІС [1, 2].

Основоположною ідеєю циклу PDCA є виконання послідовних ітерацій між діями з планування і контролю при реалізації певної діяльності (процесу) з метою її дискретного удосконалення за тими напрямками, які встановлює організація. Отже, повторювання циклу PDCA може наблизити до досягнення встановлених цілей (або ж до одержання інформації з обґрунтуванням необхідності виправданої зміни цих цілей). Причому це відбуватиметься без реалізації додаткових, спеціально розроблених процесів, а виключно завдяки вбудованому механізму самовдосконалення, закладеному у документованих процедурах, що регламентують процес.

Слід також підкреслити, що методологія PDCA застосовна практично для всіх видів проектів і процесів, де можна налагодити управління за зворотним зв’язком [10]. Підтвердженням цього є включення рекомендацій щодо застосування циклу PDCA у стандарти ISO 9001 та ISO 27001, який може використовуватись організаціями будь-якого профілю [8].

В СМІБ всі процеси ґрунтується на моделі PDCA (рис. 1.4).

1.4. Модель PDCA (Плануй - Роби - Перевіряй - Дій\Впливай)

Цикл PDCA – є широко поширеним методом безперервного поліпшення якості. Цей метод має і другу назву – колесо Демінга, через наочну кругову графічну інтерпретацію стадій циклу.

Безперервність поліпшення якості – це постійний процес вдосконалення обладнання, матеріалів, інструментів, використання людських ресурсів і виробничих технологій тощо.

Згідно з положеннями стандарту ISO 27001 СМІБ повинна мати процесний характер, що відповідає циклу Демінга-Шухарта, який передбачає таку послідовність дій: планування процесу, його реалізація, перевірка, подальші вдосконалення, що полягають у ретельному перегляді підходів з актуалізацією уваги на плануванні, згодом цикл повторюється.

Якщо уважно подивитися на зміст ISO/IEC 27001, то можна виокремити розташовані послідовно один за одним розділи стандарту (див. рис. 1.5):

– Planning (Планування);
– Operation (Функціонування);
– Performance evaluation (Оцінка результативності);
– Improvement (Поліпшення), які і відображають модель Демінга-Шухарта, або, як ще її називають, модель PDCA (Plan-Do-Check-Act).

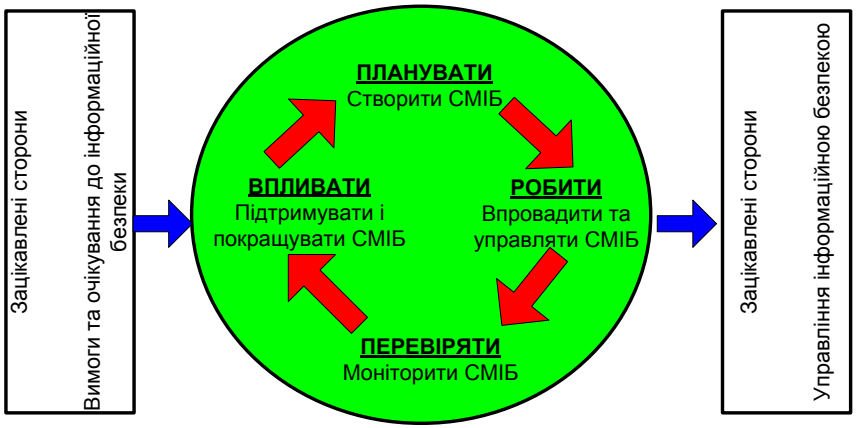


Рис. 1.5. Модель PDCA в СМІБ

Ця модель може бути застосована при структуруванні всіх процесів СМІБ в будь-якій організації. Система управління ІБ, використовує

нізація буде справлятися з дезорганізуючою подією і забезпечувати свою ІБ на запланованому рівні, орієнтуючись на схвалені керівництвом цілі щодо забезпечення безперервності ІБ.

Відповідно до вимог забезпечення безперервності ІБ організація повинна встановити, задокументувати, впровадити та забезпечувати працездатність:

а) засобів управління ІБ в рамках процесів забезпечення безперервності бізнесу або відновлення після надзвичайних ситуацій, процедур і забезпечуючих систем і інструментів;

б) процесів, процедур і здійснення змін для підтримки існуючих засобів управління ІБ поки триває негативна ситуація;

в) компенсуючи заходи для тих засобів управління ІБ, працездатність яких не може бути забезпечена при несприятливій ситуації.

В рамках контексту забезпечення безперервності бізнесу або відновлення після надзвичайної ситуації могли бути визначені конкретні процеси і процедури. Інформація, яка обробляється при виконанні цих процесів і процедур або в спеціалізованих ІС для їх підтримки, повинна бути захищена. Отже, організація повинна залучати фахівців з ІБ при розробці, впровадженні та функціонуванні процесів і процедур забезпечення безперервності бізнесу та відновлення після надзвичайної ситуації.

Впроваджені засоби управління ІБ повинні продовжувати функціонувати при виникненні несприятливої ситуації. Якщо засоби управління безпекою не здатні продовжувати забезпечувати безпеку інформації, повинні бути розроблені, впроваджені і підтримуватися в робочому стані інші засоби управління для забезпечення прийнятного рівня ІБ.

3) Верифікація, перегляд та оцінювання безперервності ІБ. Організація повинна підтверджувати розроблені та впроваджені заходи безперервності ІБ через регулярні інтервали часу для гарантування, що вони дійсні та ефективні протягом надзвичайних ситуацій.

Організаційні, технічні, процедурні зміни або зміни в процесах в контексті чи експлуатації, або забезпечення безперервності можуть вести до змін вимог безперервності ІБ. У таких випадках цілісність процесів, процедур і засобів управління ІБ повинна бути проаналізована з точки зору цих змінених вимог.

1) Планування безперервності ІБ. Організація повинна визначити свої вимоги щодо ІБ та безперервності управління ІБ в надзвичайних ситуаціях, наприклад під час кризи чи катастрофи.

Організація повинна визначити, чи забезпечується безперервність ІБ в рамках процесу менеджменту безперервністю бізнесу або ж в рамках процесу управління відновленням після надзвичайної ситуації. Вимоги ІБ повинні бути визначені при плануванні безперервності бізнесу і відновленні після надзвичайної ситуації.

За відсутності офіційно затверджених планів забезпечення безперервності бізнесу та відновлення після надзвичайної ситуації управління ІБ передбачає, що вимоги ІБ в несприятливих ситуаціях залишаються тими ж самими, що і в звичайних умовах експлуатації. Крім того, організація може здійснювати аналіз впливу аспектів ІБ на бізнес, щоб визначити відповідні вимоги, які застосовуються в несприятливих ситуаціях.

Для зниження витрат часу і зусиль на «додатковий» аналіз впливу ІБ на бізнес рекомендується визначати аспекти ІБ в рамках загального менеджменту безперервністю бізнесу або аналізу впливу на бізнес в рамках управління відновленням після надзвичайної ситуації. Це передбачає, що вимоги безперервності ІБ чітко сформульовані в рамках процесів управління безперервністю бізнесу або управління відновленням після надзвичайної ситуації.

Інформація з менеджменту безперервністю бізнесу може бути знайдена в стандартах ISO / IEC 27031, ISO 22313 і ISO 22301.

2) Реалізація безперервності ІБ. Організація повинна розробити, задокументувати, реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо ІБ під час надзвичайної ситуації.

Організація повинна гарантувати, що:

а) реалізована відповідна структура управління для підготовки до, мінімізації та впровадження відповідних заходів на дезорганізуючу подію за участю персоналу, що володіє необхідними повноваженнями, досвідом і компетентністю;

б) призначений персонал для реалізації відповідних заходів щодо інциденту з необхідною відповідальністю, повноваженнями і компетентністю для управління інцидентом і забезпечення ІБ;

в) розроблені і затверджені документовані плани, процедури відповідних заходів і відновлення, що деталізують, яким чином орга-

стовуючи як вхідні дані вимоги ІБ і очікування зацікавлених сторін, за допомогою необхідних дій і процесів видає вихідні дані – результати по забезпеченню ІБ [10].

1.6. Діяльність міжнародних організацій у сфері інформаційної безпеки

Серед міжнародних організацій, що діють в сфері ІБ і мають істотний вплив на функціонування глобальних ІС і діяльність всього інформаційного співтовариства, виділяють організації наступних типів.

1) Великі міжнародні некомерційні і неурядові організації, що об'єднують фахівців певних галузей, які існують, як правило, вже протягом багатьох років і охоплюють безліч основних напрямків розвитку комп'ютерної інженерії, електроніки та телекомунікацій, включаючи, в тому числі і певні питання забезпечення безпеки сучасних ІТ.

2) Окремі відносно невеликі організації, які спеціалізуються на більш-менш вузьких питаннях ІБ, що мають глобальне значення для всієї спільноти користувачів ІС, вони з'явилися на базі приватних компаній або дослідницьких структур протягом останнього десятиліття, коли проблеми ІБ стали особливо актуальними.

3) Спільні структури (комітети, альянси тощо), створювані (іноді тимчасово) великими компаніями (іноді за участю великих дослідних центрів, навчальних закладів та урядових структур) для вирішення певних завдань в сфері ІТ та ІБ.

Кожен з них, в свою чергу, має свої специфічні організаційні особливості, проте всі вони, як правило, вирішують завдання розробки, узгодження та подальшого поширення загальних для всієї спільноти користувачів ІС технічних і організаційних рішень, таких як:

– протоколи глобальних мереж;

– архітектура, алгоритми, протоколи публічних засобів шифрування даних;

– правила побудови глобальних мереж обміну даними та інших елементів глобальної інфраструктури ІБ.

Також важливими елементами організаційної роботи на рівні міжнародних структур є:

– організація обміну знаннями та актуальними новинами в середовищі фахівців з ІБ в таких формах, як публікація спеціалізованих періодичних видань та збірників наукових праць, організація спеціалізованих науково-практичних конференцій, семінарів та ін.;

– організація і підтримка в актуальному стані баз даних (БД) і знань, які містять відомості, необхідні користувачам ІС, адміністраторам, розробникам і іншим учасникам для забезпечення ІБ. Прикладами таких баз є БД, що містять відомості про виявлені уразливості різних програмних і апаратних платформ ІС.

Загалом організаційна робота на рівні міжнародних структур не є універсальною, і в більшості випадків останні будують свою роботу самостійно. Однак можна виділити деякі основні організаційні принципи, характерні для діяльності багатьох з них:

– принцип добровільної участі в роботі таких структур і в окремих проектах, і в усій роботі;

– принцип відкритості (доступності) результатів роботи (всіх або їх частини) для спільноти фахівців у сфері інформаційних технологій;

– принцип самофінансування.

Робота міжнародних професійних об'єднань

Робота великих міжнародних професійних (галузевих) організацій (об'єднань), як правило, має такі особливі риси.

Вона, як правило, не спрямована тільки на вирішення завдань ІБ – завдання ІБ вирішуються в комплексі з безліччю інших проблем (розвитком ІТ, побудовою телекомунікаційних систем та ін.).

Вона в певній мірі може спиратися на підтримку з боку різних державних структур.

Вона об'єднує велику кількість фахівців з різних дослідницьких, навчальних, комерційних організацій, але при цьому більшість учасників (членів) може не мати конкретних зобов'язань, що створюють необхідність здійснення внеску в роботу, досягнення певних цілей.

Основними найбільшими і найвідомішими міжнародними професійними об'єднаннями, що так чи інакше пов'язані з питаннями ІБ, є:

– ITU – International Telecommunication Union;

залежності від типу носіїв, пристроїв і стану пристроїв, наприклад, включених або вимкнених. Процедури повинні брати до уваги:

а) порядок передачі та зберігання;
б) збереження свідчень;
в) безпеку персоналу;
г) ролі та обов'язки задіяного персоналу;
д) компетентність персоналу;
е) документацію;
ж) інструктаж.

Там, де це можливо, повинна бути передбачена сертифікація або інші відповідні засоби оцінки придатності персоналу і інструментарію, для того, щоб підвищити цінність збережених свідчень.

Свідоцтва для судового розгляду можуть бути за межами організації або кордонів юрисдикції. У цих випадках має бути забезпечене наділення організації правом для збору необхідної в якості судового свідоцтва інформації. Повинні бути враховані вимоги різних юрисдикцій, щоб максимально збільшити шанси на визнання у відповідних юрисдикціях.

Ідентифікація – це процес, що включає пошук, визнання та документування можливого свідчення. Збір – це процес збирання фізичних елементів, які можуть містити потенційне свідчення.

Комплектування – це процес створення копій даних в рамках певного набору. Збереження – це процес підтримки і захисту цілісності і початкового стану потенційного свідчення. Коли інцидент ІБ виявлено вперше, неясно, чи призведе ця подія до судового розгляду. Таким чином, існує небезпека, що необхідне свідоцтво буде навмисно або випадково знищено до того, як з'ясується серйозність інциденту. Рекомендується залучати юриста або співробітника поліції на ранній стадії при будь-яких намічених діях юридичного характеру і прислухатися до порад з приводу необхідних свідчень.

Стандарт ISO / IEC 27037 містить вказівки з ідентифікації, збору, комплектування і збереження цифрових свідоцтв [1, 2].

4.13. Забезпечення безперервності бізнесу

Безперервність інформаційної безпеки

Ціль: безперервність ІБ має бути залучено в системи управління безперервністю бізнесу організації.

г) забезпечення того, що всі виконувані дії у відповідь відповідним чином зареєстровані для подальшого аналізу;

д) оповіщення про те, що має місце інцидент ІБ або його будь-яких істотних деталях іншим особам, які мають про це знати в силу службової необхідності, як в самій організації, так і в інших організаціях;

е) усунення уразливості (ей) ІБ, що викликала чи сприяла виникненню інциденту;

ж) офіційне закриття та документування інциденту, після того, як він був успішно відпрацьований. Повинен проводитися аналіз після інциденту, якщо необхідно, для виявлення причин інциденту.

Першочерговою метою заходів у відповідь на інцидент є повернення «нормального рівня безпеки» і потім ініціювання необхідного відновлення.

6) Знання з вивчення інцидентів ІБ. Знання, отримані з аналізу та розв'язання інцидентів ІБ, мають використовуватися для зменшення ймовірності чи впливу майбутніх інцидентів.

Повинні бути впроваджені механізми для забезпечення можливості кількісно визначати і відстежувати види, інтенсивність і збиток від інцидентів ІБ. Інформація, що отримується при оцінці інцидентів ІБ повинна використовуватися для виявлення повторюваних або інцидентів, які істотно впливають.

Оцінка інцидентів ІБ може вказувати на необхідність поліпшених або додаткових засобів управління для зниження частоти, розміру пошкоджень і шкоди у майбутньому або взяття до уваги при перегляді політики безпеки.

З урахуванням питань конфіденційності різні реальні історії, пов'язані з інцидентами ІБ, можуть бути використані при навчанні персоналу, як приклади, що може трапитися, як реагувати на такі інциденти і як уникнути їх у майбутньому.

7) Збирання доказів. Організація повинна визначити і використовувати процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази.

Повинні бути розроблені і потім виконуватися внутрішні процедури обробки свідчень з метою вжиття заходів дисциплінарного і юридичного характеру.

У загальному випадку ці процедури повинні забезпечувати процеси ідентифікації, збору, комплектування і збереження свідчень в

- IEEE – Institute of Electrical and Electronics Engineers;
- ACM – Association for Computing Machinery;
- W3 Consortium;
- ISSA – Information Systems Security Association;
- ISO – International Organization for Standardization;
- IETF – Internet Engineering Task Force;
- ICSA – International Computer Security Association;
- Information Systems Audit and Control Association (ISACA);
- Internet Security Alliance.

International Telecommunication Union (ITU) – Міжнародний союз електрозв'язку

ITU є найстарішою міжнародною організацією, що пов'язана з IT. Вона була заснована в 1885 році як Міжнародний телеграфний союз і отримала свою нову назву в 1934 році. В даний час ITU об'єднує 189 держав. Як стає зрозуміло з назви, основним її завданням спочатку були управління і координація діяльності в сфері передачі інформації і, зокрема, в радіозв'язку та телеграфному зв'язку. Однак із розвитком глобальних комп'ютерних мереж та інтеграцією комп'ютерних і телекомунікаційних систем, область діяльності ITU була значно розширена і в даний час включає в себе безліч питань, пов'язаних з побудовою комп'ютерних мереж, передачею цифрових даних, обробкою інформації т.ін.

Членами ITU-T є:

– державні органи влади (міністерства і відомства зв'язку окремих країн);

– наукові організації і компанії – виробники телекомунікаційного обладнання;

– регіональні та міжнародні телекомунікаційні організації.

Функціональними органами ITU-T є:

– Всесвітня асамблея зі стандартизації телекомунікацій (World Telecommunication Standardization Assembly), що проводиться кожні чотири роки, – основний керівний орган сектора стандартизації;

– Бюро стандартизації телекомунікацій (Telecommunication Standardization Bureau) – виконавчий підрозділ сектора стандартизації;

– Дослідницькі групи (всього їх 14);

– Консультативна група зі стандартизації телекомунікацій (Telecommunication Standardization Advisory Group) – допоміжний підрозділ, що здійснює координаційну роботу.

Вищим органом влади Союзу є Повноважна Конференція (Plenipotentiary Conference), збори делегацій держав – членів Союзу, що проходять раз на чотири роки. Основні виконавчі органи – Рада і Генеральний секретаріат ITU. Основні робочі підрозділи розділені на три сектори:

– сектор стандартизації зв'язку, ITU-T;
– сектор радіозв'язку, ITU-R;
– сектор розвитку електрозв'язку ITU-D.

ITU-R і ITU-D виконують окремі дослідницькі, координаційні та технічні функції (такі як, наприклад, реєстрація радіочастот або координація роботи космічних телекомунікаційних супутників), тоді як Сектор стандартизації зв'язку – ITU-T в більшій мірі відповідає за вирішення стратегічних завдань розвитку інформаційних технологій та інфраструктур і, зокрема, за розробку методик і стандартів, необхідних для всієї світової спільноти.

Основною метою роботи ITU-T є розробка універсальних рекомендацій та міжнародних стандартів, що належать до різних сфер телекомунікаційних технологій і управління телекомунікаціями. Рекомендації, що розробляються, забезпечують основу для розвитку ринку послуг зв'язку, створення сумісних технічних і організаційних систем та ін. З точки зору забезпечення ІБ найбільш значущими стали рекомендації, які стосуються серії «X – Мережі передачі даних і зв'язок відкритих систем» і, зокрема, до серії «X.8xx – Безпека».

Відповідно до Резолюції 1 Всесвітньої асамблеї із стандартизації телекомунікацій 2000-го року, була введена практика призначення Провідних дослідних груп (Lead Study Groups, LSGs) з певних питань, які вимагають одночасної координації зусиль декількох дослідницьких груп, які працюють в різних областях. Починаючи з вересня 2001 року функціонує «Дослідницька група 17: Мережі передачі даних і телекомунікаційне програмне забезпечення» («Study Group 17: Data Networks and Telecommunication Software»), утворена на основі існуючих до цього «Дослідницької групи 7» і

3) Звітування щодо слабких місць ІБ. Треба вимагати від усього найманого персоналу та підрядників, які користуються ІС та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах.

Всі співробітники і ті хто працює за контрактом повинні передавати повідомлення, що стосуються уразливостей в ІБ, контактному центру якомога швидше для того, щоб запобігти інциденти ІБ. Механізм оповіщення повинен бути настільки простим, доступним і працездатним, наскільки це можливо.

Співробітникам і тим хто працює за контрактом повинно бути рекомендовано не намагатися перевіряти передбачувану уразливість захисту. Тестування уразливості може бути сприйнято як можливе неналежне застосування системи і може викликати також пошкодження в ІС або сервісі та привести до юридичної відповідальності особи, яка здійснювала тестування.

4) Оцінювання та прийняття рішення стосовно подій ІБ. Події ІБ має бути оцінено та прийнято рішення стосовно віднесення їх до інцидентів ІБ.

Контактний центр повинен оцінювати кожну подію ІБ, використовуючи узгоджену класифікаційну шкалу подій та інцидентів ІБ та приймати рішення, чи повинна подія бути розцінена як інцидент ІБ. Класифікація та розподіл інцидентів за пріоритетами може допомогти у визначенні впливу і масштабу інциденту.

У тому випадку, якщо в організації є група реагування на інциденти ІБ (ISIRT), оцінка і прийняття рішення можуть бути передані їй для підтвердження або повторної оцінки. Результати оцінки та рішень повинні бути детально зафіксовано з метою звернення до них в майбутньому і перевірки.

5) Реагування на інциденти ІБ. Реагування на інциденти ІБ має здійснюватися відповідно до задокументованої процедури.

Відповідні заходи на інциденти ІБ повинні прийматися призначеним контактним центром та іншими відповідними особами в самій організації чи в інших організаціях.

Відповідні заходи повинні включати наступне:

а) якомога швидший збір свідчень того, що сталося;

б) проведення ретроспективного аналізу, якщо потрібно;

в) передача рішення на більш високий рівень, якщо це необхідно;

3) посилання на офіційно встановлений процес прийняття дисциплінарних заходів до працівників, які допустили порушення безпеки;

4) працездатні процеси зворотного зв'язку, що гарантують, що особи, які відповідають за звітність про події ІБ, повідомлені про результати після рішення і закриття проблеми.

Завдання з управління інцидентами ІБ повинні бути погоджені з керівництвом і має бути забезпечено розуміння особами, відповідальними за управління інцидентами ІБ, пріоритетів організації в рамках обробки інцидентів.

Інциденти ІБ можуть бути і не локалізовані в межах організації або держави. Для вжиття заходів у відповідь на такі інциденти є необхідність в їх координації та обмін інформацією про ці інциденти з іншими організаціями, в тій мірі, наскільки це можливо.

Докладне керівництво з управління інцидентами ІБ дано в ISO / IEC 27035.

2) Звітування про події ІБ. Необхідно якнайшвидше звітувати стосовно подій ІБ через належні канали управління.

Всі співробітники і ті хто працює за контрактом повинні бути ознайомлені зі своїм обов'язком повідомляти про події ІБ як можна швидше. Вони повинні також знати процедури передачі повідомлення про події ІБ та контакти, за якими повідомлення про подію має бути передано.

Ситуації, які передбачають передачу повідомлення про подію ІБ, включають в себе:

а) не результативний контроль безпеки;

б) порушення очікуваного рівня цілісності, конфіденційності або можливості застосування інформації;

в) людські помилки;

г) невідповідності політикам та інструкціям;

д) порушення заходів фізичної безпеки;

е) неконтрольовані зміни систем;

ж) збої в роботі ПЗ або технічних засобів;

з) порушення доступу.

Збої або інша невідповідна поведінка системи можуть бути індикаторами атаки на систему захисту або порушення захисту і, отже, про них завжди необхідно повідомляти як про події ІБ.

«Дослідницької групи 10» . З моменту свого утворення вона є Провідною дослідницькою групою з питань безпеки комунікаційних систем (Communication Systems Security, CSS) і, відповідно, не тільки працює над забезпеченням безпеки технологій, що безпосередньо належить до її компетенції, а й займається питаннями забезпечення безпеки різних комунікаційних технологій, що розробляються іншими дослідницькими групами.

Однією з найбільш значущих розробок цієї групи в сфері інформаційної безпеки вважається Стандарт X.509, що заклав основи розвитку інфраструктури публічних ключів. Найбільш актуальними проблемами, над якими в даний час працює Провідна дослідницька група з питань безпеки комунікаційних систем, є:

– управління безпекою;
– безпека мобільних систем;
– безпека систем зв'язку служб реагування на надзвичайні ситуації;
– телебіометрія.

Загалом робота цієї дослідницької групи охоплює такі основні сфери:

– безпеку управління мережами (включає в себе роботу над наступними рекомендаціями: M.3010 – Принципи мереж управління телекомунікаціями, M.3016 – Огляд безпеки мереж управління телекомунікаціями і деякі інші);
– аутентифікацію і служби каталогів (X.500 – Огляд концептуальних моделей і сервісів, X.509 – Основи технології публічних ключів і сертифікатів і деякі інші);
– управління системами (X.733 – Функція звіту про подію, X.740 – Функція проведення аудиту безпеки і деякі інші);
– основи архітектури безпеки (X.800 – Архітектура безпеки інфраструктури відкритих систем для додатків ITU; X.802 – Модель безпеки нижніх рівнів, X.803 – Модель безпеки верхніх рівнів і деякі інші);
– факсимільний зв'язок (т.36 – Можливості забезпечення безпеки при використанні факсимільних апаратів третьої групи; T.563 – Характеристики терміналів для використання з факсимільними апаратами четвертої групи і деякі інші);

– телевізійні та кабельні системи (J.170 – Специфікація безпеки IPCabelcom і деякі інші);

– техніка забезпечення безпеки (X.841 – Об'єкти ІБ для контролю доступу та деякі інші);

– мультимедійні комунікації (H.233 – Система забезпечення конфіденційності для аудіовізуальних сервісів, H.234 – Управління ключами шифрування і системою аутентифікації в аудіовізуальних сервісах і деякі інші).

Крім розробки рекомендацій і стандартів, одним з важливих напрямків роботи ITU стало також забезпечення інформаційного обміну в різних формах: поширення методичних матеріалів, що стосуються забезпечення ІБ, проведення семінарів і конференцій. Одним з таких найбільш масштабних заходів є Всесвітній саміт з інформаційного суспільства (WSIS: The World Summit On The Information Society).

Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки

IEEE є однією з найбільш відомих професійних організацій. Вона існує з 1884 року і в даний час налічує близько 380000 членів з 150 країн світу. У сферу її інтересів входить безліч питань, пов'язаних з електротехнікою, радіоелектронікою, обчислювальною технікою, інформатикою, а також деякими розділами фізики і математики. Основні напрямки роботи цієї організації:

– проведення спеціалізованих професійних конференцій;

– публікація спеціалізованих видань;

– підтримка освітньої діяльності;

– підтримка інноваційних технічних і методичних розробок в різних сферах;

– розробка та розповсюдження технічних стандартів.

До складу IEEE входять 10 регіональних відділень, 38 професійних товариств, 4 ради і 1450 студентських відділень. Поточне управління діяльністю на верхньому рівні здійснюється Радою директорів і Виконавчим комітетом, роботу яких очолюють Президент та Виконавчий директор.

Одним з основних підрозділів IEEE, що спеціалізуються на питаннях ІБ, є Технічний комітет з безпеки і захисту приватної інформації – «IEEE Computer Society Technical Committee on Security

5) процедури для оцінювання та прийняття рішення за подією ІБ, а також оцінці уразливостей в інформаційному захисті;

6) процедури відповідних заходів, включаючи передачу інформації для прийняття рішення на більш високому рівні, керованого відновлення після інциденту і інформування як персоналу всередині організації, так і осіб за її межами;

б) встановлена процедура повинна гарантувати, що:

1) проблеми, пов'язані з інцидентами ІБ, вирішує компетентний персонал;

2) контактний центр з питань виявлення та інформування про інциденти безпеки діє;

3) відповідні контакти з повноважними органами, зовнішніми зацікавленими групами або форумами, які присвячені питанням, пов'язаним з інцидентами ІБ, підтримуються;

Рис. 4.14. Управління інцидентами ІБ

в) процедури звітності повинні включати в себе:

1) розробку форм звітності про події ІБ для забезпечення дій з інформування та полегшення співробітнику виконання всіх необхідних заходів, якщо відбулася подія ІБ;

2) процедуру, яка повинна бути виконана, якщо відбулася подія ІБ, наприклад, негайне повідомлення всіх подробиць, таких, як вид невідповідності або порушення, відмову, що сталася, екранні повідомлення і негайне інформування контактного центру, а також прийняття тільки скоординованих дій;

4.12. Управління інцидентами інформаційної безпеки

Інцидент ІБ – одинична, небажана або несподівана подія ІБ (або сукупність таких подій), яка може скомпрометувати бізнес-процеси компанії або загрожує її ІБ **(**ISO / IEC TR 18044).

Важливо, щоб жоден інцидент не залишився непоміченим!

Інцидентами ІБ можуть бути:

а) відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання;

б) порушення конфіденційності та цілісності цінної інформації;

в) недотримання вимог ІБ, прийнятих в компанії (порушення правил обробки інформації);

г) незаконний моніторинг ІС;

д) шкідливі програми;

е) компрометація ІС (наприклад, розголошення пароля користувача);

ж) неавторизована зміна даних на сайті компанії;

з) залишення комп'ютера незаблокованим без нагляду;

и) пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти.

Управління інцидентами ІБ та вдосконаленням

Ціль: гарантувати послідовний та ефективний підхід до управління інцидентами ІБ (див. рис. 4.14), охоплюючи поширення інформації про події безпеки та слабкі місця.

1) Відповідальності та процедури. Має бути визначено відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти ІБ.

Повинні бути прийняті до уваги наступні рекомендації для встановлення обов'язків керівництва і процедур, пов'язаних з управлінням інцидентами ІБ:

а) повинні бути встановлені обов'язки керівництва, щоб гарантувати, що такі процедури розроблені та організація відповідним чином про них повідомлена:

1) процедури планування та підготовки реакції на інцидент;

2) процедури моніторингу, виявлення, аналізу та інформування про події та інциденти ІБ;

3) процедури реєстрації дій з управління інцидентами;

4) процедури управління свідченнями для суду;

and Privacy» (http://www.ieee-security.org/). У його складі функціонують три підкомітети:

– Підкомітет із стандартів (Subcommittee on Standards);

– Підкомітет з академічної роботи (Subcommittee on Academic Affairs);

– Підкомітет із спеціалізованих конференцій (Subcommittee on Security Conferences).

Основними заходами, які проводить цей комітет, є:

– Щорічний симпозіум з безпеки і захисту приватної інформації (IEEE CS Symposium on Security and Privacy);

– Щорічний семінар з основ ІБ (Computer Security Foundations Workshop).

Також комітет веде роботу зі збору та узагальнення актуальної інформації про події в співтоваристві фахівців з ІБ: оголошення про заплановані конференції, звіти про минулі конференції і семінари, огляди літератури та періодики, посилання на ресурси в мережі Інтернет і т.п.. Спеціальний інформаційний бюлетень з цією інформацією – «Cipher» – розсилається передплатникам в середньому один раз в два місяці.

Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки

Асоціація ACM є однією з найстаріших організацій, пов'язаних з IT, вона була заснована в 1947 році, на зорі розвитку комп'ютерної техніки. Основні завдання ACM – підтримка освітніх проектів в сфері IT, організація науково-практичних конференцій, симпозіумів та семінарів, суспільно-політична робота, пов'язана з IT, публікація періодичних видань і збірників наукових праць, присвячених проблемам сучасних IT, підтримка електронного архіву таких публікацій, а також інша подібна діяльність. Основним керуючим органом цієї організації є Рада ACM, в яку входить 16 осіб, в тому числі президент і віце-президент. Управління поточними справами Асоціації здійснюють чотири профільні комітети. Штаб-квартира ACM, в якій працюють основні виконавчі органи, розташовується в Нью-Йорку починаючи з 1960 року.

Однією з основ організації роботи ACM є поділ всієї спільноти членів асоціації на так звані групи спеціальних інтересів (Special Interests Group – SIG) – підрозділи, які спеціалізуються на окремих

відносно вузьких проблемах розвитку інформаційних технологій. Усього ACM об'єднує 34 групи, які спеціалізуються на різних питаннях розробки і використання програмного забезпечення (ПЗ), апаратних засобів і телекомунікацій. Кожна з груп самостійно визначає для себе межі своєї діяльності, а їхня політика та фінансові питання координуються одним із комітетів.

Одна з цих груп – Special Interest Group on Security, Audit and Control (SIGSAC, Група спеціальних інтересів з питань безпеки, аудиту і контролю, http://www.acm.org/sigs/sigsac/) – спеціалізується на питаннях ІБ. Основним завданням цієї групи є організація роботи спеціалізованих науково-практичних конференцій, таких як:

– Симпозіум з технологій і моделей управління доступом (SACMAT: ACM Symposium on Access Control Models and Technologies), що проводиться щорічно починаючи з 1995 року;

– Конференція з безпеки комп'ютерів і комунікацій (CCS: ACM Conference on Computer and Communications Security), що проводиться щорічно починаючи з 1993 року.

Крім того, питання ІБ прямо або побічно торкаються в роботі інших спеціалізованих груп Асоціації, таких як, наприклад, Special Interest Group on Electronic Commerce (Група з проблем електронної комерції).

World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини

Створення W3C було ініційовано в 1989 році з метою розробки єдиних, узгоджених стандартів обміну інформацією в глобальних мережах передачі даних, а офіційно створення консорціуму було оформлено в 1994 р. Його основними завданнями є:

– забезпечення можливості доступу до мережі Інтернет для якомога більшої кількості людей незалежно від знання іноземних мов, культурної приналежності, географічного положення та доступних їм технічних засобів і технічної інфраструктури;

– забезпечення можливості підключення до Інтернет різних технічних пристроїв;

– забезпечення можливості структурування і формалізації інформації, доступної через Інтернет, з метою зробити її якомога більш придатною для автоматизованої обробки;

постачальникам встановлений обов'язок з аналізу відповідності та забезпечення виконання вимог угоди. Повинні бути виділені достатні ресурси з необхідними технічними навичками для моніторингу того, що вимоги угоди, зокрема, вимоги ІБ, виконуються. Необхідно вжити відповідних заходів при виявленні недоліків в наданні послуг.

Організація повинна зберігати достатній загальний контроль і обізнаність з усіх аспектів безпеки щодо уразливої або критично важливої інформації або пристроїв обробки інформації, до яких постачальник має доступ, використовує або управляє.

Організація повинна зберігати обізнаність про дії, пов'язані з безпекою, такими, як управління змінами, виявлення уразливостей, а також оповіщення про інциденти ІБ і заходи у в рамках встановленого процесу інформування.

2) Управління змінами у послугах постачальника. Зміни в наданні послуг постачальника, зокрема й підтримування та вдосконалювання наявних політик ІБ, процедур і заходів безпеки, мають управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків.

Повинні бути прийняті до уваги такі аспекти:

а) зміни в угодах з постачальниками;

б) зміни, що здійснюються організацією для здійснення:

1) поліпшення пропонованих у даний момент послуг;

2) розробки будь-яких нових додатків і систем;

3) зміни або оновлення політик і процедур організації;

4) нових або змінених засобів управління для вирішення інцидентів ІБ та поліпшення захисту;

в) зміни в послугах постачальника з метою:

1) зміни і поліпшення мереж;

2) застосування нових технологій;

3) введення нових продуктів або нових версій / релізів;

4) застосування нових інструментів і середовищ розробки;

5) зміни фізичного місцезнаходження обслуговуючого обладнання;

6) зміни постачальників;

7) укладення контакту з іншим субпідрядником [1, 2].

Ланцюжок поставки інформаційно-комунікаційних технологій, як вона тут розуміється, включає в себе і послуги хмарних технологій.

Управління наданням послуг постачальником

Ціль: Підтримувати належний рівень ІБ та надання послуг відповідно до угод з постачальниками.

1) Моніторинг та перегляд послуг постачальника. Організація повинна регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника.

Моніторинг і аналіз послуг постачальника повинен гарантувати, що положення з ІБ і умови угод виконуються і що інциденти і проблеми у сфері ІБ вирішуються належним чином.

Це повинно реалізовуватися через процес взаємодії між організацією і постачальником при управлінні послугами, щоб:

а) відстежувати рівень виконання послуги для контролю відповідності угодам;

б) вивчати звіти про послугу, що подаються постачальником, і організовувати регулярні робочі наради, як це визначено угодами;

в) проводити аудити постачальників разом з аналізом звітів незалежних аудиторів, якщо вони є, і здійснювати наступні дії щодо виявлених проблем;

г) отримувати інформацію про інциденти ІБ і аналізувати цю інформацію, як вимагається угодами, і будь-якими робочими інструкціями і процедурами;

д) аналізувати контрольні журнали постачальників і записи про події ІБ, експлуатаційних проблемах, збої, виявленні причин помилок і порушень, пов'язаних з послугами, що поставляються;

е) вирішувати будь-які виявлені проблеми;

ж) аналізувати взаємовідносини постачальника з його підрядниками у частині ІБ;

з) гарантувати, що постачальник забезпечує свою здатність надавати послуги на належному рівні при наявності працездатних планів, розроблених щоб забезпечити узгоджені рівні безперервності надання послуги при значних збоїв і аварійних ситуаціях в ході надання послуги.

Відповідальність за управління взаємовідносинами з постачальниками повинна бути покладена на конкретну особу або групу з управління послугами. Крім того, організації слід гарантувати, що

– забезпечення надійності та безпеки обміну інформацією, а також можливості брати участь в інформаційному обміні з тим рівнем захищеності, який окремі користувачі вважають для себе достойним.

І до тепер консорціум об'єднує понад чотириста провідних технологічних і телекомунікаційних компаній, урядових організацій, дослідницьких центрів, інститутів і університетів по всьому світу. Крім того, в штаті консорціуму перебувають близько 70 незалежних технічних експертів, які забезпечують його роботу. Фінансування діяльності здійснюється за рахунок членських внесків, а основні адміністративні функції і повсякденна діяльність виконуються на базі трьох організацій:

1) Массачусетський технологічний інститут (США);

2) Європейський консорціум з досліджень у галузі інформатики та математики (Франція);

3) Університет Кейо (Японія).

Крім формування стандартів («рекомендацій»), ця організація також займається освітньою діяльністю і надає можливості для обговорення різних питань, пов'язаних з функціонуванням Інтернет.

Діяльність консорціуму організована у вигляді груп: Робочі групи (займаються вивченням технічних питань), Групи спеціальних інтересів і Координаційні групи (забезпечують взаємодію між іншими групами). У кожну групу входять представники організацій-учасників консорціуму і запрошені експерти. Сфери роботи консорціуму («домени», Domain), розділені на напрями (Activities). Робота по двадцяти чотирьох напрямках виконується в цілому шістдесятьма групами.

Питаннями ІБ займається сфера «Технологія і суспільство» (Technology and Society Domain) в рамках спеціального напряму «Безпека» (W3C Security Activity), що складається з двох робочих груп. Також до 2006 року в складі Консорціуму функціонував напрямок «Захист приватної інформації» (Privacy).

До робіт консорціуму в сфері ІБ відносяться:

– розробка стандарту цифрових підписів для інформаційних ресурсів (PICS Signed Labels 1.0 Specification);

– розробка системи електронного підпису для документів XML;

– розробка стандартів передачі зашифрованих даних з використанням мови XML.

International Organization for Standardization (ISO) – Міжнародна організація по стандартизації

ISO в сучасному вигляді була заснована в 1946 р. і являє собою неурядове об'єднання національних організацій по стандартизації, націлене на уніфікацію стандартів (головним чином, технічних) в різних областях виробничої діяльності та надання послуг.

Крім основних членів (156 країн), що безпосередньо беруть участь в роботі, в ISO також входять члени-кореспонденти (Correspondent member) – країни, які не мають повноцінних органів стандартизації, а також члени-передплатники (Subscriber member) – країни з невеликими економіками, які отримують необхідну довідкову інформацію на пільгових умовах.

Головним органом управління ІСО є щорічна Генеральна Асамблея, яка приймає стратегічні рішення, що стосуються розвитку всієї організації. Підготовкою матеріалів для прийняття таких рішень займається Рада ІСО, збори якої проходять два рази на рік. Безпосередньо розробкою стандартів займаються технічні комітети і підкомітети, в роботі яких беруть участь представники зацікавлених країн. За розробку кожного документа в підкомітеті відповідає спеціально створена для цього робоча група. Проекти міжнародних стандартів, прийняті технічними комітетами, розсилаються в національні організації для голосування; документ набуває статусу міжнародного стандарту, якщо за нього проголосувало не менше 75% членів, які брали участь в голосуванні.

У 2006 році Керівне технічне бюро ISO (ISO/ TMB) заснувало Технічну координаційну групу (JTCG) для координації розроблення стандартів ISO на системи управління з метою підвищення їхньої послідовності та сумісності [11].

Склад JTCG. Усі технічні комітети ISO (TCs), підкомітети (SCs), проектні комітети (PCs) або робочі групи (WGs), відповідальні за розроблення стандартів на системи управління або словників, беруть участь у роботі JTCG, а також у Комітеті з оцінювання відпо-

г) виконання процесу моніторингу та відповідних методів для підтвердження, що їх товари та послуги у сфері інформаційно-комунікаційних технологій відповідають встановленим вимогам;

д) виконання процесу визначення компонентів продукту або послуги, які важливі для підтримки функціональності і, таким чином, вимагають підвищеної уваги і вивчення, якщо створені за межами організації, особливо, якщо первинний постачальник передає на аутсорсинг виробництво якихось елементів продукту або послуги іншим постачальникам;

е) отримання впевненості у тому, що критично важливі компоненти і їх походження можна простежити по всьому ланцюжку поставки;

ж) отримання впевненості в тому, що продукти та послуги у сфері інформаційно-комунікаційних технологій, які поставляються функціонують очікуваним чином і не мають будь-яких непередбачених або небажаних функцій;

з) визначення правил обміну інформацією, що стосуються ланцюжка постачання і будь-яких можливих проблем та взаємних поступок між організацією і постачальниками;

и) виконання конкретних процесів управління життєвим циклом компонентів інформаційно-комунікаційних технологій, а також доступністю і ризиками, пов'язаними з безпекою. Це включає в себе управління ризиками щодо компонентів, які більш не доступні в силу того, що їхні постачальники припинили свою діяльність, або припинили постачання цих компонентів через розвитку технологій.

Конкретні методи менеджменту ризику в ланцюжку поставки інформаційно-комунікаційних технологій засновані на високорівневих процедурах забезпечення загальної ІБ, якості, управління проектами та розробки систем, але не замінюють їх.

Організаціям рекомендується співпрацювати з постачальниками, щоб мати розуміння всього ланцюжка постачання інформаційно-комунікаційних технологій і будь-яких питань, які мають значний вплив на їх товари та послуги.

Організації можуть впливати на методи забезпечення ІБ в ланцюжку поставок інформаційно-комунікаційних технологій чіткою регламентацією в угодах зі своїми постачальниками питань, які слід вирішити постачальникам по всьому ланцюжку поставки інформаційно-комунікаційних технологій.

о) процеси усунення дефектів і вирішення спорів;

п) зобов'язання постачальника періодично надавати незалежний звіт про результативність засобів управління і згоду на своєчасне рішення відповідних проблем, згаданих у звіті;

р) зобов'язання постачальника відповідати вимогам ІБ організації.

Угоди можуть істотно відрізнятися для різних організацій і різних видів постачальників. У зв'язку з цим слід приділити увагу тому, щоб врахувати всі значимі ризики, пов'язані з ІБ, і вимоги. Угоди з постачальниками можуть також допускати участь інших сторін (наприклад, субпідрядників). В угоді повинні бути передбачені процедури забезпечення безперервності виробничих процесів, щоб уникнути будь-яких затримок у заміні продуктів і послуг в разі, якщо постачальник перестає бути здатним постачати ці продукти або послуги.

3) Ланцюг постачання інформаційних та комунікаційних технологій. Угоди з постачальниками мають містити вимоги стосовно адресації ризиків ІБ, пов’язаних з ланцюгом постачання продуктів та послуг інформаційних і комунікаційних технологій.

Відносно безпеки ланцюжків поставок повинні бути розглянуті для включення в угоди з постачальниками наступні положення:

а) визначення вимог ІБ, які можна застосувати до закупівель продуктів і послуг у сфері інформаційно-комунікаційних технологій, а також загальних вимог ІБ, що належать до взаємин з постачальниками;

б) вимога для послуг у сфері інформаційно-комунікаційних технологій, щоб постачальники поширювали вимоги організації, пов'язані з безпекою, на весь ланцюжок постачання, якщо постачальник залучає підрядників для виконання якоїсь частини послуг у сфері інформаційно-комунікаційних технологій, що надаються організацією;

в) вимога для продуктів у сфері інформаційно-комунікаційних технологій, щоб постачальники поширювали відповідні процедури, пов'язані з безпекою, на весь ланцюжок постачання, якщо ці продукти містять у собі компоненти, що купуються у інших постачальників;

відності (ISO/CASCO). Сьогодні JTCG складається із представників таких комітетів:

– ISO/JTC1/SC 27 – управління інформаційною безпекою;
– IS0/TC 8 – управління безпекою ланцюга постачання;
– ISO/TC 34 – управління безпекою харчових продуктів;
– ISO/TC 176 (+ SC 1, SC 2, SC 3) – управління якістю;
– ISO/TC 207 (+ SC 1, SC 2, JTG) – управління навколишнім середовищем;
– ISO/TC 223 – оперативне управління безперервністю;
– ISO/PC 241 – управління безпекою дорожнього руху;
– ISO/PC 242 – управління енергетикою;
– ISO/TMB/WG – управління ризиками;
– ISO/CASC0 – Комітет з оцінювання відповідності.

Керівництво JTCG змінюється кожні два роки.

Основним підрозділом ІСО, які займаються питаннями ІБ, є Об'єднаний технічний комітет JTC 1 «Інформаційні технології», до складу якого входить підкомітет SC 27 «Засоби безпеки в IT» (IT Security techniques), в свою чергу до нього входять 5 робочих груп (див. рис. 1.6). За час своєї роботи цей підкомітет розробив понад 60 міжнародних стандартів, що відносяться до ІБ.

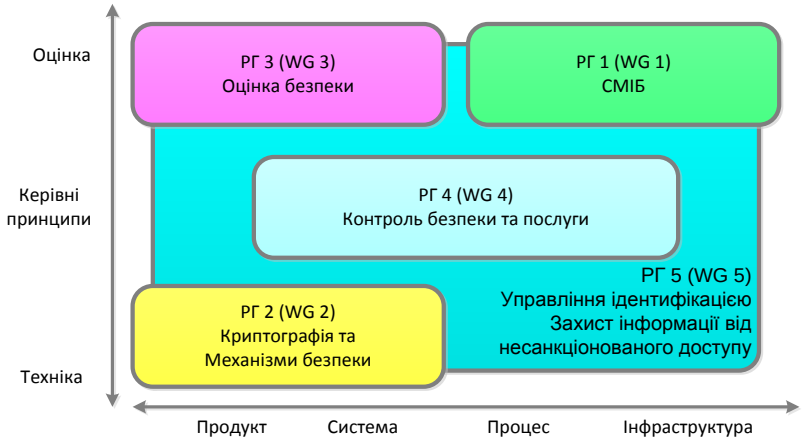


Рис. 1.6. Робочі групи в межах підкомітету
ISO / IEC JTC 1 / SC 27 – Технології безпеки IT

З питаннями ІБ також пов'язана робота підкомітету SC 37 «Біометрична ідентифікація» (Biometrics) і підкомітету SC 17 «Картки і персональна ідентифікація» (Cards and personal identification).

1.7. Діяльність спеціалізованих міжнародних організацій і об'єднань в сфері інформаційної безпеки

Спеціалізовані організації, що мають глобальний вплив на управління ІБ на різних рівнях і на загальний стан ІБ, як правило, можуть функціонувати на базі:

– приватних компаній, що займаються дослідженнями, розробками та консультуванням у сфері ІБ;

– великих навчальних закладів, що спеціалізуються на ІТ, а також володіють істотним авторитетом і фінансовими ресурсами;

– урядових установ, відповідальних за забезпечення ІБ у певних сферах.

Основним напрямком організаційної роботи, що здійснюється в такій формі, стає формування та підтримка баз даних, що містять інформацію про віднайдені уразливості різних програмних і апаратних засобів, а також інші форми і напрямки інформаційної, консультативної та методичної роботи в даній сфері. Важливими чинниками успішності функціонування таких організацій є об'єднання інформації з якомога більшої кількості джерел (зокрема, від якомога більшої кількості фахівців і компаній, що займаються проблемами інформаційної безпеки) і якнайбільш ефективне поширення відомостей (знань) в співтоваристві користувачів ІС.

З огляду на те, що така форма організаційної роботи заснована на приватних компаніях і відносно невеликих установах, підходи до організації та управління зазвичай не підкоряються будь-яким загальним правилам. Також склад таких організацій може з часом змінюватися: на зміну одним дослідницьким центрам можуть приходити інші – більш успішні та ефективні – з тими ж функціями. У даний час можна виділити наступні найбільш значущі організації, що займають цю нішу:

– CERT Coordination Center - Координаційний центр CERT;

– Дослідницька група X-Force компанії IBM.

Для виконання встановлених вимог ІБ слід розглянути з точки зору включення в угоди наступні положення:

а) визначення наданої інформації або інформації, до якої надається доступ, а також методи надання інформації або доступу до інформації;

б) категорії інформації відповідно до схеми класифікації організації. Зіставлення, якщо необхідно, схем класифікації організації і постачальника;

в) законодавчі та нормативні вимоги, включаючи вимоги до захисту даних, прав інтелектуальної власності та авторських прав, а також опис того, яким чином буде гарантовано їх виконання;

г) зобов'язання кожної сторони контракту виконувати узгоджений набір засобів управління, включаючи контроль доступу, контроль виконуваних робіт, моніторинг, звітність та аудити;

д) правила допустимого застосування інформації, включаючи опис неприпустимого;

е) або повний перелік співробітників постачальника, яким дано доступ до інформації або право отримувати інформацію від організації, чи процедури або умови для отримання такого дозволу, а також анулювання дозволу доступу чи права отримання інформації організації персоналом постачальника;

ж) політики ІБ відповідно до конкретного контракту;

з) вимоги з управління інцидентами і процедури (особливо оповіщення та спільної роботи з усунення наслідків інциденту);

и) ознайомлення та навчання виконанню вимог конкретних процедур і вимог ІБ, наприклад, відповідних дій щодо інциденту, процедур авторизації;

к) відповідні регламенти для підрядників, включаючи засоби управління, які повинні виконуватися;

л) відповідні контактні особи за угодою, включаючи контактну особу з питань ІБ;

м) вимоги до попередньої перевірки персоналу постачальника, якщо такі встановлені, включаючи обов'язки з проведення процедур попередньої перевірки та інформування в разі, коли перевірка не була завершена або її результати дають підстави для сумнівів або побоювань;

н) право на аудит процесів постачальника і здійснення процедур контролю, пов'язаних з контрактом;

з) обробку інцидентів і непередбачених наслідків, пов'язаних з доступом постачальника, включаючи зобов'язання як організації, так і постачальника;

и) здатність до відновлення і, якщо необхідно, заходи з відновлення та аварійні заходи для забезпечення доступності інформації або обробки інформації, які вживаються будь-якою зі сторін;

к) ознайомлення персоналу організації, що бере участь у закупівлях, з діючими політиками, процесами і процедурами;

л) ознайомлення персоналу організації, що взаємодіє з персоналом постачальників, з відповідним правилами взаємодії і поведінки з урахуванням виду постачальника і рівня його доступу до систем організації та інформації;

м) умови, при яких вимоги з ІБ і засоби управління будуть включені в угоду, підписану обома сторонами;

н) управління необхідною передачею інформації, пристроїв обробки інформації і чим-небудь ще, що мають потребу в передачі, і гарантія того, що безпека забезпечується протягом усього періоду передачі.

При неналежному управлінні безпекою можуть виникати ризики з боку постачальників. Повинні бути визначені і виконуватися заходи для управління доступом постачальників до пристроїв обробки інформації. Наприклад, якщо існує особлива необхідність в збереженні конфіденційності інформації, може укладатись угода про нерозголошення. Інший приклад захисту даних від ризиків, коли угода з постачальниками включає в себе питання передачі за кордон або доступу до інформації з-за кордону. Організація повинна пам'ятати, що відповідальність за дотримання законодавства та контрактних зобов'язань лежить на самій організації.

2) Врахування безпеки в угодах з постачальниками. Усі відповідні вимоги щодо ІБ має бути встановлено та погоджено з кожним постачальником, який може мати доступ, обробляти, зберігати, передавати чи надавати компоненти ІТ-інфраструктури для інформації організації.

Угоди з постачальниками повинні бути розроблені і документовані з гарантією, що немає розбіжностей між організацією і постачальником щодо взаємних зобов'язань щодо виконання відповідних вимог ІБ.

CERT Coordination Center (CERT / CC) – Координаційний центр CERT

CERT / CC, що виникла в 1988 році як Computer security incident response team (Група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує на базі Інституту розробки програмного забезпечення при Університеті Карнегі-Мелон (Software Engineering Institute, Carnegie Mellon University) і фінансується Міністерством оборони і Міністерством національної безпеки США. Поряд з проведенням незалежних досліджень та рішенням різних завдань із забезпечення безпеки глобальної інформаційної інфраструктури, ця організація забезпечує централізований збір відомостей про всі слабкі місця в різних ІС і підтримку актуальної бази знань про уразливість в ІС. Відомості про знову виявлені слабкі місця, шкідливі програми і способи порушення ІБ розсилаються на електронну пошту: передплатниками цього бюлетеня є більш ніж 161000 фахівців у всьому світі.

В рамках цієї діяльності CERT / CC здійснює постійну дослідницьку роботу:

– визначення характеру можливих наслідків використання виявлених уразливостей і вірусів;

– аналіз наявних засобів використання уразливостей;

– аналіз того, наскільки активно використовуються уразливості і наскільки широко поширені віруси;

– взаємодія з постачальниками ІС з метою більш глибокого аналізу виявлених уразливостей.

На основі проведеного аналізу CERT / CC розробляє заходи щодо усунення уразливостей і рекомендації по зменшенню негативних наслідків. За результатами цієї роботи всім передплатникам розсилається інформація про загрози ІБ і можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова та технічна документація, проводиться подальша дослідницька та методична робота. Зокрема, CERT / CC підтримує програму безпечної розробки ПЗ («secure coding»), що ґрунтується на тому, що велика частина уразливостей виникає в наслідок відносно невеликого числа помилок в програмному коді ІС. Таким чином, CERT / CC на основі накопичених результатів аналізу уразливостей веде цілеспрямовану роботу по виявленню типових програмних поми-

лок, виробленню стандартів безпечного програмування і поширенню цієї інформації серед розробників ПЗ.

Крім основної інформаційної роботи з уразливими, CERT також займається супутніми видами діяльності:

– організацією навчальних курсів з різних напрямків (мережева безпека, управління інформаційними ризиками, організація роботи груп реагування);

– сертифікацією фахівців з реагування на інциденти в сфері ІБ;

– підтримкою фундаментальних наукових досліджень в різних галузях ІБ, таких як методи розробки безпечних додатків, виявлення уразливостей, аналіз шпигунського ПЗ, вирішення питань безпеки як складова частина процесу розробки і т. ін.;

– сприянням розвитку локальних (національних і корпоративних) груп реагування на інциденти.

X-Force security intelligence team – Дослідницька група X-Force

Діяльність цієї групи є одним з напрямків бізнесу компанії Internet Security Systems (ISS) – найбільш авторитетного постачальника комплексних рішень в сфері ІБ, клієнтами якого є всі без винятку найбільші компанії США, а також урядові організації. В кінці 2006 року ISS була куплена компанією IBM і інтегрована в неї в якості самостійного підрозділу. Одним із завдань групи X-Force є підтримка в актуальному стані БД відомих уразливостей різних програмних і апаратних платформ. База даних, підтримувана цією групою, доступна в мережі інтернет і постійно поповнюється відомостями про нові уразливості (в даний час їх налічується понад 40000). Основні причини, за якими дана організація є провідною в цій області, такі:

– велика кількість великих компаній-клієнтів, від яких постійно надходить інформація про напади, уразливості тощо;

– наявність власної науково-дослідної бази, на основі якої постійно здійснюється виявлення нових уразливостей і узагальнення відомостей про уразливість, отриманих з різних джерел;

– використання спеціально розроблених універсальних класифікацій (зокрема, загального словника найменувань

4.11. Відносини з постачальниками

Інформаційна безпека у взаємовідносинах з постачальниками

Ціль: гарантувати захист ресурсів СМІБ організації, які можуть бути доступні постачальникам.

1) Політика ІБ для взаємовідносин з постачальниками. Вимоги ІБ для послаблення ризиків, пов’язаних із доступом постачальників до ресурсів СМІБ організації має бути погоджено з постачальником та задокументовано.

Організація повинна в політиці визначити і зробити обов'язковими засоби управління ІБ, які відносяться саме до доступу постачальників до інформації організації. Ці засоби управління повинні визначати процеси та процедури, які повинні виконуватися організацією, а також ті процеси і процедури, які організація повинна вимагати виконувати від постачальника, включаючи:

а) визначення та документування видів постачальників, наприклад, IT-послуги, доставки, фінансових послуг, компоненти IT-інфраструктури, які будуть мати доступ до її інформації;

б) стандартизований процес і модель життєвого циклу для управління відносинами з постачальниками;

в) визначення видів доступу до інформації, які будуть дозволені для різних видів постачальників, а також доступу з метою моніторингу та контролю;

г) мінімальні вимоги з ІБ для кожного виду інформації та вид доступу для визначення основних положень угоди з конкретним постачальником, що враховують бізнес-потреби організації і вимоги, а також характер ризиків;

д) процеси і процедури для моніторингу дотримання встановлених вимог щодо ІБ для кожного виду постачальників і виду доступу, включаючи перевірку та затвердження продукції третьою стороною;

е) коректність і повноту засобів управління для забезпечення цілісності інформації або обробки інформації, що проводиться будь-якою стороною;

ж) види зобов'язань, які можна застосувати до постачальників для ЗІ організації;

Приймальне тестування системи повинне включати в себе перевірку виконання вимог з ІБ і дотримання встановлених правил безпечної розробки систем. Тестування повинне проводитися також для отриманих компонентів та вбудованих систем. Організації можуть застосовувати автоматизовані засоби, такі як аналізатори коду або сканери уразливостей, і повинні перевіряти виправлення пов'язаних з безпекою дефектів. Тестування повинне виконуватися у реалістичному тестовому середовищі, щоб гарантувати, що система, яка перевіряється не в несе уразливостей в інфраструктуру організації та що результати тестування надійні.

Дані для тестування системи

Ціль: забезпечити захист даних, які використовують для тестування.

Захист даних для тестування системи. Дані для тестування мають бути ретельно відібрані, захищені та контрольовані.

Слід уникати використання у цілях тестування інформацію, що містить особисті дані людини, або будь-яку іншу конфіденційну інформацію. Якщо ж інформація, що містить особисті дані людини, або якась інша конфіденційна інформація використовується для цілей тестування, то всі конкретні подробиці і дані повинні бути видалені або змінені (див. ISO / IEC 29101).

Для захисту робочих даних, що використовуються з метою тестування, рекомендується застосовувати такі рекомендації:

а) процедури контролю доступу, що застосовуються в діючих прикладних системах, слід також застосовуватися і в системах тестування застосунків;

б) щоразу, коли робоча інформація копіюється в середовище тестування, слід застосовувати окрему авторизацію;

в) робоча інформація повинна бути видалена з середовища тестування негайно після того, як тестування завершено;

г) копіювання та використання робочої інформації повинно реєструватися, щоб забезпечити можливість перевірки.

Системне і приймальне тестування зазвичай вимагає значних обсягів тестових даних, максимально близьких до робочих даними [1, 2].

уразливостей – Common Vulnerabilities and Exposures, CVE) для зберігання і обробки інформації в БД відомих уразливостей.

Також одним з напрямків довідково-інформаційної діяльності цієї дослідницької групи є надання послуг по індивідуальному аналізу загроз і інформування (X-Force Threat Analysis Service (XFTAS)). Даний комплекс послуг дозволяє замовникам щодня отримувати адаптовану актуальну інформацію про погрози і уразливості з урахуванням особливостей побудови їх ІС (платформ, додатків, сфери ведення бізнесу, географічного положення) і включає в себе:

- інформацію про загрози;
- експертний аналіз загроз;
- опис поточного і прогнозованого стану загроз;
- рекомендовані способи усунення загроз;
- кількісний аналіз атак за останні 30 днів.

Ще одним із завдань групи є випуск періодичних (щоквартальних, щорічних) інформаційних бюлетенів з оглядами найбільш значущих подій в сфері ІБ.

Альянси великих технологічних компаній

Спільні альянси (асоціації, коаліції, групи) великих (іноді середніх) технологічних і консультаційно-дослідницьких компаній представляють собою тимчасові (які укладаються на короткострокову або середньострокову перспективу) або довгострокові угоди між декількома фірмами, спрямовані на спільне, скоординоване, цілеспрямоване вирішення певних масштабних і ресурсоємних завдань розвитку технології, формування ринкового попиту на певні продукти і організацію інфраструктури ІБ. Велике значення такої форми організаційної роботи в сфері ІБ, як формування альянсів великими і середніми компаніями, що спеціалізуються на ІТ, обумовлене тим, що:

- такі альянси здатні здійснити найбільші інвестиції в розробку нових технологій і проведення досліджень, які можуть вплинути на весь розвиток ІТ і стан справ в сфері ІБ;
- компанії, що входять в такі альянси, займають значну частку ринку і тому визначають загальний напрямок розвитку ІТ взагалі і засобів ЗІ зокрема;

– такі альянси компаній здатні створити комплексні технології, продукти і рішення, що охоплюють різні аспекти функціонування ІС і засобів ЗІ, і таким чином досягти нового рівня захищеності інформації, що практично неможливо при роботі компаній (навіть найбільших) окремо.

Як правило, кожен такий альянс є унікальним, і учасники в кожному конкретному випадку визначають умови роботи в рамках такої організаційної форми. На конкретний підхід до організації альянсу можуть вплинути такі фактори, як:

– характер цілей і завдань, які постають перед альянсом;

– поточний стан справ в тій області, для роботи в якій створюється альянс;

– склад учасників альянсу, їх роль і місце на ринку ІТ;

– наявність можливих конкурентів (наприклад, аналогічних альянсів паралельно створюються іншими групами компаній);

– взаємовідносини, які раніше склалися між компаніями – учасниками альянсу, та інші.

Завданнями формування альянсів можуть бути:

– розробка нових продуктів і послуг, а також базових технологій, протоколів, алгоритмів і угод, на основі яких такі продукти і послуги в майбутньому могли б розроблятися;

– формування нових ринків збуту і підтримка існуючих;

– вплив на державні та громадські організації, а також на співтовариство користувачів ІС з метою забезпечення розвитку і більш широкого використання ІТ і засобів ІБ;

– вплив на систему професійної підготовки фахівців з метою забезпечення якості їх навчання.

Основними типовими прийомами організаційної роботи на такому рівні є:

– скоординований вибір і уніфікація технічних рішень (апаратних пристроїв, програмних алгоритмів), які використовуються в системах передачі та обробки інформації та / або СЗІ;

– інформаційна підтримка як виробників ІС і постачальників рішень (що входять в альянс і не входять в нього), так і споживачів і користувачів (потенційних і реальних);

в) забезпечення зовнішнього постачальника затвердженою моделлю загроз;

г) приймальне тестування для забезпечення якості та коректності поставлених товарів;

д) забезпечення свідоцтва того, що були застосовані порогові критерії безпеки для встановлення мінімально прийнятних рівнів захищеності і конфіденційності;

е) забезпечення свідоцтва того, що було виконане тестування в достатньому обсязі, щоб підтвердити відсутність навмисного або ненавмисного шкідливого вмісту у продуктах, які поставляються;

ж) забезпечення свідоцтва того, що було виконане тестування в достатньому обсязі, щоб підтвердити відсутність відомих уразливостей;

з) угоду про умовне депонування, якщо вихідний код більше недоступний;

и) обумовлені контрактом права на аудит процесів розробки і засобів управління нею;

к) діюча документація на середовище збірки, яка використовується для формування продуктів, що поставляються;

л) організація залишається відповідальною за відповідність чинному законодавству і перевірку ефективності контролю.

Додаткова інформація з взаємовідносин з постачальниками може бути знайдена в ISO / IEC 27036.

8) Тестування безпеки системи. Тестування функціональності безпеки потрібно виконувати протягом розроблення.

Нові та оновлюванні системи вимагають ретельного тестування і перевірки в ході процесів розробки, включаючи підготовку детального графіку робіт, вихідних даних для тестування та очікуваних в деякому діапазоні умов результатів. При розробці власними силами такі тести повинні спочатку виконуватися командою розробників. Потім має виконуватися незалежне приймальне тестування (як для розробки власними силами, так і для переданої на сторону), щоб гарантувати, що система працює як очікувалося і тільки так. Обсяг тестування повинен відповідати важливості і характеру системи.

9) Приймальне тестування системи. Програми приймального тестування та відповідні критерії має бути визначено для нових ІС, оновлень та нових версій.

проектування для розроблення систем та інтеграції зусиль, що покривають повний життєвий цикл розроблення системи.

Безпечне середовище розробки включає в себе персонал, процеси і технології, пов'язані з розробкою та інтеграцією систем. Організація повинна оцінювати ризики, пов'язані з певними діями з розробки систем, і формувати безпечні середовища розробки для конкретних робіт з розробки систем, беручи до уваги:

а) уразливість даних, що підлягають обробці, зберіганню і передачі в системі;

б) діючи зовнішні і внутрішні вимоги, наприклад, регламенти або політики;

в) засоби управління безпекою, вже впроваджені організацією для забезпечення розробки систем;

г) сумлінність персоналу, що працює в даному середовищі;

д) ступінь передачі на сторону робіт, пов'язаних з розробкою систем;

е) необхідність поділу різних середовищ розробки;

ж) контроль доступу до середовища розробки;

з) моніторинг змін, як самого середовища розробки, так і коду, розміщеного в ньому;

и) резервні копії, які зберігаються на віддалених захищених майданчиках;

к) контроль переміщення даних як у, так і з середовища розробки.

Як тільки організація визначила рівень захисту для конкретного середовища розробки, вона повинна документувати відповідні процеси в процедурах забезпечення безпеки розробки і забезпечити цими процедурами всіх, кому вони необхідні.

7) Аутсорсингове розроблення. Організація повинна здійснювати нагляд над аутсорсинговим розробленням систем та його моніторинг.

Якщо розробка системи передана на аутсорсинг, для всіх учасників ланцюжка поставки організації повинні враховуватися такі моменти:

а) ліцензійні угоди, права на код і інтелектуальну власність, пов'язані із технічною характеристикою на стороні контенту;

б) контрактні вимоги щодо безпечного проектування, кодування і тестування;

– скоординований розподіл функцій по розробці окремих елементів ІТ в рамках спільної узгодженої стратегії розвитку;

– скоординована маркетингова та інформаційна політика, спрямована на забезпечення використання (підтримки, сумісності) створюваних рішень (технологій, протоколів т. ін.) якомога більшою кількістю споживачів і незалежних виробників, а також її визнання урядовими структурами;

– спільний вплив на органи державної влади (лобіювання) з метою забезпечення державною підтримкою певних продуктів, проектів, технологій і архітектур ІС і СЗІ.

Smart Card Alliance (SCA) – Альянс за смарт-картками

SCA (http://www.smartcardalliance.org) займається питаннями розвитку технології смарт-карт – однією з ключових технологій в сфері ІБ, що використовується для ідентифікації користувачів різних сервісів і ІС (таких як мобільні телефонні мережі, банківські «електронні гаманці» тощо). Цей довгостроковий (стратегічний) альянс був утворений на початку 2001 року шляхом злиття двох організацій: Smart Card Industry Association і Smart Card Forum. До складу альянсу входять близько сотні різних компаній і урядових організацій. При цьому в складі учасників альянсу виділяються кілька груп:

– Керівна Рада (Leadership Council) – провідні компанії, що визначають основну політику Альянсу: Visa USA, Bank of America, IBM, Lockheed Martin, Intel, Mastercard International і деякі інші (всього більше двадцяти компаній);

– основна група членів Альянсу – різні фірми, так чи інакше пов'язані з питаннями ІБ, постачанням відповідних продуктів і послуг (такі як Texas Instruments Incorporated, Sun Microsystems та інші) – всього близько 70 компаній;

– члени – урядові організації. У цю групу входять як федеральні урядові установи США (Державний департамент, Міністерство національної безпеки та інші), так і місцеві органи влади (Портова адміністрація Нью-Йорка, Транспортна адміністрація Вашингтона та інші) – всього близько 30 членів.

Також до складу Альянсу входить один університет і кілька асоційованих членів.

Роботу альянсу очолюють Рада директорів і Виконавчий директор. Діяльність альянсу розподілена на членські ради (Member Council) за окремими сферами інтересів:

– Рада з безконтактних і мобільних платежів;
– Рада з охорони здоров'я (спеціалізується на питаннях використання смарт-карт в сфері охорони здоров'я);
– Рада з ідентифікації;
– Рада з систем контролю за фізичним допуском;
– Рада із транспорту (спеціалізується на питаннях просування і адаптації смарт-карт в транспортній сфері).

Кожна рада управляється керівником, віце-керівниками і керуючим комітетом.

Напрямки роботи Альянсу включають в себе:

– організацію спеціалізованих щорічних конференцій;
– організацію освітніх програм і системи сертифікації фахівців;
– видання різних інформаційних і довідкових матеріалів як технічного, так і управлінського характеру;
– ведення централізованої бази даних постачальників обладнання та послуг в сфері смарт-карт.

Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет

ISA був створений в квітні 2001 року з ініціативи двох великих авторитетних організацій: CERT/CC Університету Карнегі-Меллон і Асоціації електронної промисловості (Electronic Industries Alliance, EIA). Вже до середини 2004 року в альянс входило близько тридцяти членів, в числі яких такі великі компанії, як Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec і інші. Роботою Альянсу керує Рада директорів, до якої входять авторитетні представники найбільш відомих компаній-членів. Крім того, до складу альянсу входять близько тридцяти асоційованих членів. На початковому етапі створення альянсу його основним завданням було підвищення ефективності обміну інформацією про уразливість, яка поширюється CERT/CC. Надалі коло завдань альянсу розширювалося, і тепер робота ведеться за наступними напрямками:

встановлені для всього дозволеного до зміни ПЗ. Всі зміни повинні бути повністю протестовані і документовані так, щоб вони могли бути зроблені повторно, якщо необхідно, в ході подальших оновлень ПЗ. Якщо потрібно, то зміни повинні бути протестовані і схвалені незалежним випробувальним центром.

5) Принципи проектування безпечної системи. Принципи проектування безпечних систем потрібно розробити, задокументувати, виконувати та використовувати для будь-яких зусиль щодо реалізації ІС.

Повинні бути розроблені, задокументовані і застосовуватися у корпоративній діяльності з розробки ІС процедури розробки захищених ІС, засновані на принципах безпечної розробки. Захист повинен бути вбудований на всіх архітектурних рівнях (бізнес, дані, застосунки і технологія), забезпечуючи баланс між необхідністю ЗІ та вимогами до доступності. Нові технології повинні аналізуватися в плані ризиків для безпеки. Проектні рішення повинні розглядатися з точки зору відомих моделей атак.

Ці принципи і встановлені процедури розробки повинні регулярно переглядатися з тим, щоб вони сприяли результативному розвитку стандартів безпеки в рамках процесів розробки. Вони повинні також регулярно переглядатися для гарантії того, що вони залишаються актуальними в плані боротьби з будь-якими потенційними новими загрозами і придатними в світлі удосконалень для використовуваних технологій і рішень.

Встановлені принципи безпечної розробки повинні застосовуватися, там, де це можливо, для ІС, переданих на аутсорсинг, через контракти та інші зобов'язуючі угоди між організацією і постачальником. Організація повинна підтверджувати, що строгість принципів безпечної розробки постачальника порівнянна з її власною.

Процедури розробки додатків повинні використовувати методи безпечного проектування в розробці застосунків, що мають інтерфейси введення-виведення. Методи безпечного проектування забезпечують методичну основу для методів авторизації користувачів, управління захистом сесії і підтвердження правильності даних, видалення налагоджувальних кодів.

6) Безпечне середовище розроблення. Організації повинні запровадити та відповідним чином захистити безпечне середовище

так як деякі оновлення можуть викликати падіння критичних застосунків.

3) Технічний перегляд прикладних програм після змін операційної платформи. Коли операційні платформи змінено, критичні для бізнесу прикладні програми має бути переглянуто й протестовано, щоб забезпечити відсутність негативного впливу на функціонування та безпеку організації

Цей процес повинен охоплювати:

а) перегляд процедур контролю та забезпечення цілісності застосунків для гарантії того, що вони не були порушені при змінах операційних платформ;

б) гарантію того, що оповіщення про зміни операційного середовища зроблено своєчасно, даючи можливість провести відповідні тести і аналіз до початку впровадження;

в) гарантію того, що зроблені відповідні зміни в планах по безперервності бізнесу.

Операційні платформи включають в себе ОС, бази даних та проміжне ПЗ. Повинен також застосовуватися контроль змін застосунків.

4) Обмеження на зміни до пакетів ПЗ. Модифікації пакетів ПЗ не повинні заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни потрібно суворо контролювати.

Наскільки це можливо і практично здійснено, ПЗ, що купується у постачальника повинно використовуватися без змін. У тих випадках, коли програмний пакет вимагає змін, повинні прийматися до уваги наступні моменти:

а) ризик порушення вбудованих засобів управління і процесів забезпечення цілісності;

б) має бути отримана згода постачальника;

в) можливість отримання необхідних змін від постачальника як штатного оновлення програми;

г) наслідки того, що після внесення змін організація стане відповідальною за подальшу підтримку ПЗ;

д) сумісність з іншим використовуваним ПЗ.

Якщо зміни необхідні, то оригінал ПЗ повинен залишитися незачепленим, а зміни внесені у вибраний екземпляр. Повинен виконуватися процес управління оновленням ПЗ, щоб гарантувати, що більшість актуальних узгоджених патчів і оновлень додатків

– створення ефективних механізмів обміну інформацією про уразливість в мережі інтернет і знайденими рішеннями проблем безпеки;

– дослідження фундаментальних проблем безпеки;

– розвиток програм професійної підготовки і сертифікації фахівців з ІБ;

– взаємодія з державними органами законодавчої та виконавчої влади.

The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування

Асоціація була створена в 1998 році з метою колективної підтримки інтересів компаній, пов'язаних з виробництвом біометричного устаткування. Основним завданням альянсу є взаємодія з потенційними замовниками їхньої продукції (як серед комерційних компаній, так і в громадському секторі) з метою просування засобів біометричної ідентифікації. Членами асоціації є близько 30 компаній і організацій, серед яких Hitachi, LG Electronics, Panasonic, NEC та інші.

Управління поточними справами здійснює Рада директорів у складі одинадцяти чоловік, а також виконавчий директор. Діяльність Асоціації розподілена на шість робочих груп, серед яких:

– робоча група зі стандартів і технологій. Її основна мета – захищати базові інтереси членів альянсу в сфері стандартизації біометричних технологій і систем, що використовують біометрію;

– робоча група із споживчих додатків. Займається орієнтацією ринку споживчих систем на більш широке використання біометричних технологій;

– робоча група з міжнародних ринків. Здійснює контакти з іншими біометричними організаціями по всьому світу;

– робоча група з утворення, маркетингу та інформування. Забезпечує інформаційну присутність компаній-членів асоціації в різних областях через реалізацію маркетингових заходів і освітніх програм;

– робоча група із глобальної політики. Проводить інформаційну роботу з представниками урядових структур по всьому світу [12].

1.8. Серія стандартів ISO/IEC 27000. Історія стандарту ISO/IEC 27001

Міністерство торгівлі і промисловості Великобританії (DTI) організувало робочу групу для розробки серії кращих практик щодо забезпечення безпеки. У 1989 році DTI опублікувало стандарт User Code of Practice. Цим стандартом був перелік засобів управління безпекою, які в той час вважалися адекватними, нормальними і хорошими, з можливістю застосування як до технологій, так і до середовищ того часу.

Розвиток ІС на початку 90-х років призвів до необхідності розробки нових стандартів з управління безпекою. За запитом британського уряду і промисловості, британський департамент торгівлі і промисловості розробив Практики до СМІБ. У розробці цього документа брали участь British Telecom, Marks and Spencer, National Westminster Bank, Nationwide, Shell UK, Shell International, Unilever (рис. 1.7).

1995

– Поява британського стандарту BS 7799-1: 1995. Частина 1, яка описує принципи і структуру СМІБ, включає в себе список елементів управління, який був набором кращих практик для забезпечення ІБ.

1998

– Поява нової редакції BS 7799-1: тисяча дев'ятсот дев'яносто вісім.

– Поява стандарту BS 7799-2: 1998. Частина 2 – Вимоги до СМІБ. Друга частина стандарту була додана як BS 7799: 1998, частина 2. Метою частини 2 було створення інструментарію для вимірювання і управління Частиною 1 і створення критерію для сертифікації. З цього моменту з'явилася можливість проводити сертифікацію по британському стандарту.

1999

– Поява нової редакції BS 7799-1: 1999.

– Поява нової редакції BS 7799-2: 1999.

Процедури управління змінами повинні включати, але не обмежуватися, наступне:

а) ведення записів про узгоджені рівнях авторизації;

б) гарантію того, що зміни підтверджені авторизованими користувачами;

в) аналіз засобів управління і цілісності процедур, щоб гарантувати, що вони не будуть порушені змінами;

г) виявлення ПЗ, інформації, елементів баз даних і устаткування, які вимагають змін;

д) виявлення і перевірка критичного з точки зору безпеки коду для мінімізації ймовірності реалізації відомих загроз безпеки;

е) отримання формального схвалення деталізованих пропозицій до початку роботи;

ж) гарантію, що зміни схвалені до їх реалізації авторизованими користувачами;

з) гарантію того, що комплект системної документації оновлений після закінчення кожної зміни і що попередні версії документів поміщені в архів або знищені;

и) підтримку контролю версій для всіх змін ПЗ;

к) ведення контрольних записів по всім запитам на зміни;

л) гарантію того, що робоча документація і призначені для користувача процедури змінені таким чином, щоб залишитися відповідними;

м) гарантування того, що здійснення змін проводиться в належний момент часу і не перешкоджає виконанню бізнес-процесів, яких торкається.

Зміна ПЗ може впливати на операційне середовище і навпаки.

Гарна практика, яка має на меті тестування нового ПЗ у середовищі, відокремленому як від середовища розробки, так і від робочого середовища. Це забезпечує механізми контролю нового ПЗ і можливість додаткового захисту робочої інформації, яка використовується для цілей тестування. Це також відноситься до патчів, сервіс-пакам і іншим оновлень.

Там, де передбачається автоматичне оновлення, повинен бути оцінений ризик для цілісності та готовності системи в порівнянні з виграшем у швидкості розгортання оновлення. Не повинно використовуватися автоматичне оновлення для критичних систем,

д) захищені репозиторії;

е) безпеку при управлінні версіями;

ж) необхідні знання про безпеку додатків;

з) здатність розробників уникати, виявляти і усувати уразливості.

Повинні використовуватися безпечні методи програмування як для нових розробок, так і для кодування повторно використовуваних фрагментів, для яких невідомі використані при їх розробці стандарти або ж вони несумісні з поточною практикою. Повинні бути передбачені стандарти безпечного кодування і, де це важливо, вони повинні бути обов'язковими. Розробники повинні бути навчені застосуванню цих стандартів і тестуванню, а аналіз коду повинен служити перевіркою їх застосування. Якщо розробка віддана на аутсорсинг, організація повинна отримати гарантії, що зовнішня сторона відповідає вищенаведеним правилам безпечної розробки.

Розробка може вестися засобами самих застосунків, таких як офісні пакети, скриптові мови, браузери або бази даних.

2) Процедури контролю змін системи. Зміни в системах всередині життєвого циклу розроблення мають бути контрольованими за допомогою офіційно оформлених процедур контролю змін.

Повинні бути задокументовані і виконуватися процедури управління змінами, щоб гарантувати цілісність системи, застосунків і продуктів, від ранніх стадій проектування до всіх подальших дій з підтримки.

Впровадження нових систем і великих змін в існуючі системи має відбуватися відповідно до формалізованого процесу документування, специфікації, тестування, контролю якості та керованої реалізації.

Цей процес повинен включати в себе оцінку ризику, аналіз впливу змін і визначення необхідних засобів управління безпекою. Цей процес також повинен гарантувати, що існуючі процедури захисту і управління не порушені, що програмісти, які здійснюють підтримку, мають доступ тільки до тієї частини системи, яка необхідна для їх роботи і що офіційне узгодження і схвалення для будь-яких змін отримані.

Там, де це можливо, процедури управління змінами для застосунків і операційного середовища повинні бути об'єднані.

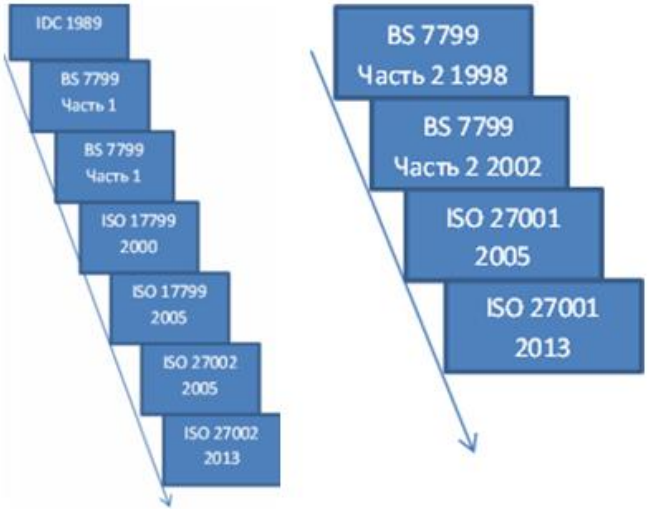


Рис. 1.7. Розробка стандартів ISO 27001 та ISO 27002

2000

– Поява міжнародного стандарту ISO 17799: 2000. З цього моменту стандарт BS 7799-1:1999 отримав міжнародне визнання.

2001

– Поява нової редакції BS 7799-2: 2001.

2002

– Поява нової редакції BS 7799-2: 2002.

2003

– Національний Банк Молдови висунув вимоги до комерційних банків щодо запровадження СМІБ на основі ISO 17799: 2000.

2004

– Білорусія прийняла ГОСТ 17799.

– Центральний банк Росії на базі ISO 17799 2000 створив стандарт управління ІБ для банківської сфери.

2005

– З'явився стандарт ISO / IEC 27001: 2005, який замінив BS 7799-2: 2002.

– Поява нової редакції ISO 17799: 2005.

2006

– Росія працює над перекладом стандартів ISO 17799: 2005 та ISO 27001: 2005.

– У Росії і Україні з'явилися фахівці з розробки СМІБ.

– Підприємства країн СНД ведуть роботи по розробці СМІБ.

– Міжнародні органи сертифікації отримали акредитацію на право проведення сертифікації.

– На початку 2006 р. британці вводять новий стандарт в галузі управління ризиками ІБ – BS 7799-3, який у подальшому отримає індекс 27005.

2007

– В цьому році стандарт ISO 27001, безумовно, став стандартом де-факто для систем управління ІБ.

– Найбільш значущою подією в Росії стає вихід ГОСТу 17799. Правда поки цей ГОСТ є перекладом стандарту ISO 17799: 2000. Ведеться робота над перекладами і скоро очікується вихід ГОСТ 17799: 2005 і ГОСТ 27001.

– Число компаній в світі, які отримали офіційний сертифікат – понад 3500.

– У Росії 6 компаній отримали сертифікати. В інших країнах СНД (Вірменія, Молдова) – 2 сертифіковані компанії. Число компаній в СНД, що знаходяться в стадії підготовки до сертифікації – більш 10.

– В Україні 1 компанія, яка отримала сертифікат.

2008

– Покладено початок робіт в Україні з випуску ДСТУ ІСО 17799 і ДСТУ ІСО 27001.

2011

– НБУ прийняв ISO / IES 27001: 2005 та ISO / IES 27002: 2005 галузевими банківськими стандартами.

Згідно зі статтею 7 Закону України «Про Національний банк України» та статтею 10 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», з метою підвищення

1) секретна інформація для автентифікації користувачів є перевіреною і діючої;

2) операція залишається конфіденційною;

3) зберігається конфіденційність для всіх сторін-учасниць;

в) канали зв'язку між сторонами є шифрованими;

г) протоколи для обміну даними між сторонами є захищеними;

д) гарантію того, що зберігання подробиць операції здійснюється за межами загальнодоступної зони, наприклад, на платформах зберігання, існуючих у внутрішній мережі організації, і ця інформація не зберігається і не копіюється на носії, безпосередньо доступні з Інтернету;

е) в тих випадках, коли використовується довірений центр сертифікації (наприклад, з метою випуску та підтримки цифрових підписів або цифрових сертифікатів) захист є комплексним і вбудований у наскрізний процес управління підписами/сертифікатами.

Ступінь обраного контролю повинен бути порівнянний з рівнем ризику, пов'язаного з кожною конкретною формою операції прикладної послуги.

Для операцій може вимагатися відповідність законодавчим і нормативним вимогам в рамках тієї юрисдикції, де операція генерується, відбувається, завершується і зберігається.

Безпека в процесах розроблення та підтримки

Ціль. Гарантувати, що ІБ проектують та впроваджують протягом життєвого циклу розроблення ІС.

1) Політика безпечного розроблення. Потрібно встановлювати та застосовувати до розробників всередині організації правила для розроблення ПЗ та систем.

Безпечна розробка є вимогою при побудові захищених сервісів, архітектури, ПЗ і систем. В рамках політики безпечної розробки повинні бути враховані наступні аспекти:

а) безпечне середовище розробки;

б) керівні вказівки щодо забезпечення безпеки протягом життєвого циклу розробки:

1) безпечна методологія розробки ПЗ;

2) керівництво з безпечного кодування для кожної використовуваної мови програмування;

в) вимоги щодо безпеки на стадії проектування;

г) контрольні точки перевірки безпеки в рамках етапів проекту;

л) дії для уникнення втрат або дублювання інформації за операціями;

м) відповідальність, пов'язану з шахрайськими операціями;

н) вимоги з страхування.

Багато рекомендацій з перерахованих вище можуть бути виконані за допомогою застосування криптографічних методів, з урахуванням відповідності вимогам законодавства.

Відносини в сфері прикладних послуг між партнерами повинні підтримуватися документованою угодою, яка встановлює зобов'язання обох сторін за узгодженими умовами застосування послуг, включаючи деталі авторизації.

Повинні бути прийняті до уваги вимоги стійкості до атак, які можуть включати вимоги щодо захисту використовуваних серверів застосунків, або гарантію доступності між мережевих з'єднань, необхідних для виконання послуг.

Застосунки, доступні через мережі загального користування, схильні до ряду загроз, таких як шахрайська діяльність, порушення умов договору або публічне розкриття інформації. Тому обов'язкові детальна оцінка ризиків і відповідний вибір засобів управління. Необхідні засоби управління часто включають в себе криптографічні методи для автентифікації і безпечної передачі даних. Прикладні послуги можуть використовувати безпечні автентифікаційні методи, наприклад, застосування криптографії з відкритим ключем або цифрових підписів, для зниження ризиків. Також можуть бути задіяні довірені треті сторони там, де такі послуги необхідні.

3) Захист транзакцій прикладних сервісів. Інформація, залучена в транзакції прикладних сервісів, має бути захищена для запобігання неповній передачі, неправильній маршрутизації, несанкціонованій зміні повідомлення, несанкціонованому розголошенню, несанкціонованому дублюванню повідомлення чи його повторенню.

Фактори, що враховуються при захисті операцій, здійснюваних при користуванні прикладними послугами, повинні включати наступне:

а) використання електронних підписів кожною стороною, яка бере участь в операції;

б) всі аспекти операції, тобто забезпечення того, що

рівня інформаційної безпеки в банківській системі України Правління Національного банку України постановляє:

1. Ввести в дію такі галузеві стандарти України (далі – галузеві стандарти): ДСТУ СУІБ 1.0 / ISO / IES 27001: 2010 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги »(ISO / IES 27001: 2005, MOD); ГСТУ СУІБ 2.0 / ISO / IES 27002: 2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (ISO / IES 27002: 2005, MOD).

2. Департаменту інформатизації (А.С. Савченко) протягом 10 днів після державної реєстрації цієї постанови в Міністерстві юстиції України довести його зміст і галузеві стандарти до відома банків України для керівництва і використання в роботі.

3. Банкам України впровадити галузеві стандарти до 01.01.2011.

Стандарт BS 7799 пройшов довгий шлях, з низкою випробувань і коригувань. Найважливішим етапом в його «кар'єрі» став 2005 рік. У 2005 році стандарт, що дозволяє оцінювати СМІБ був визнаний міжнародним. Це означає, що міжнародна спільнота підтвердила спроможність вимог стандарту до сучасної СМІБ. З цього моменту передові підприємства в усьому світі активно почали впровадження стандарту ISO 27001 та підготовку до сертифікації.

Серія стандартів ISO / IEC 27000

ISO і Міжнародна електротехнічна комісія (МЕК, IEC) спільно розробляють міжнародні стандарти і керівництва. Однією з їхніх спільних цілей є випуск стандартів з менеджменту безпеки. Робота по формуванню стандартів здійснюється на колективній основі, в ній беруть участь Робоча група 1 (WG1), Робоча група 2 (WG2) і Робоча група 3 (WG3). Всі ці робочі групи входять до складу Підкомітету 27 (SC27), який, в свою чергу, входить до Спільного технічного комітету 1 (JTC1). Робоча група 1 працює над створенням стандартів управління безпекою, включаючи розробку нових стандартів ІБ і стандартів СМІБ.

Мета цієї робочої групи – забезпечити наявність орієнтирів, які будуть вказувати вимоги до майбутнього набору міжнародних стандартів та настанов щодо створення, впровадження, експлуатації, моніторингу та підтримки СМІБ. В рамках цієї мети в ISO / IEC вирішили змінити нумерацію для міжнародних стандартів з ІБ на

нову – 27000 – сімейство міжнародних стандартів на СМІБ (див. рис. 1.8.). Це сімейство включає в себе Міжнародні стандарти, що визначають вимоги до СМІБ, управління ризиками, метрики і вимірювання, а також керівництво із впровадження. Для цього сімейства стандартів використовується послідовна схема нумерації, починаючи з 27000 і далі.

Проекти міжнародних стандартів, прийняті спільним технічним комітетом, передаються в державні органи для голосування. Публікація в якості міжнародного стандарту вимагає схвалення від не менше ніж 75 відсотків державних органів, які проголосували. Міжнародні стандарти проектуються відповідно до правил, встановлених Директивами ISO / IEC, Частина 2.

Переклад міжнародних стандартів управління ІБ російською мовою і їх поширення на території Росії і країн СНД здійснюється компанією GlobalTrust – офіційним дистриб'ютором Британського інституту стандартів (BSI) на основі ліцензії BSI [13].

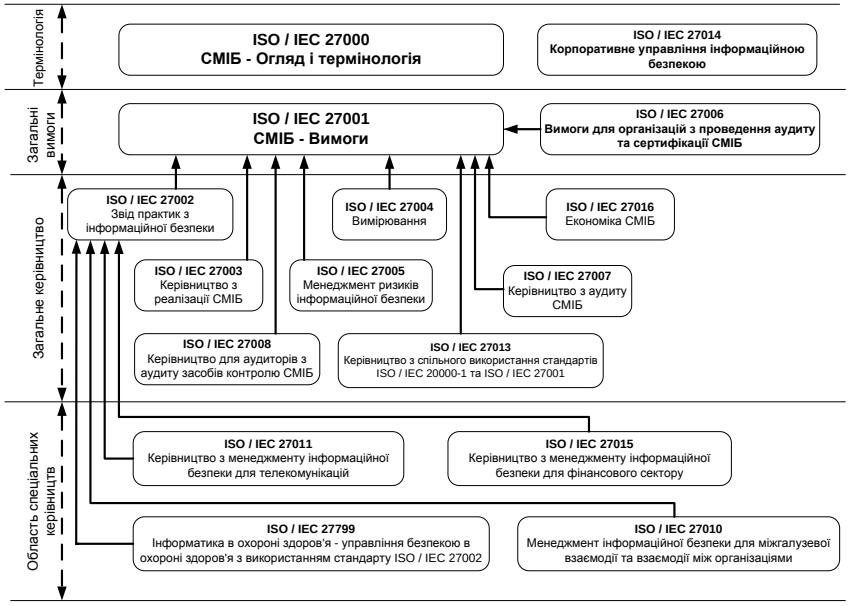


Рис. 1.8. Міжнародні стандарти лінійки СМІБ

тує, що встановлені вимоги щодо захисту будуть виконані. Продукти повинні бути оцінені за цими критеріями до придбання.

Додаткова функціональність повинна бути проаналізована, щоб гарантувати, що вона не несе будь-яких додаткових неприйнятних ризиків.

Стандарти ISO / IEC 27005 і ISO 31000 містять керівництво з застосування процесів ризик-менеджменту до визначення засобів управління для виконання вимог щодо ІБ.

2) Безпечні прикладні сервіси в публічних мережах. Інформація в прикладних сервісах, яку передають через публічні мережі, має бути захищеною від шахрайської діяльності, контрактних суперечок, несанкціонованого розголошення та модифікації.

Фактори, що враховуються при ЗІ, використовуваного прикладними послугами, що передається по загальнодоступних мереж, повинні включати наступне:

а) рівень надійності, який кожна сторона вимагає від пропонованої іншою стороною ідентифікаційної інформації, наприклад, за допомогою автентифікації;

б) процеси санкціонування, пов'язані з особами, які можуть схвалити зміст, випуск або підписати ключові ділові документи;

в) гарантію того, що партнери з обміну інформацією повністю інформовані про їхні права з надання і використання послуг;

г) визначення та виконання вимог щодо конфіденційності, цілісності, підтвердження відправки та отримання ключових документів, а також з незаперечності авторства контрактів, наприклад, пов'язаних з тендерними або договірними процесами;

д) рівень довіри, необхідний для впевненості в цілісності ключових документів;

е) вимоги щодо захисту особистої інформації;

ж) конфіденційність і цілісність будь-якої передачі даних зі замовлення, платежу, адреси поставки і підтвердженню отримання;

з) рівень перевірки, що забезпечує підтвердження платіжної інформації, наданої замовником;

и) вибір найбільш придатних форм розрахунків для захисту від шахрайства;

к) рівень захисту, необхідний для забезпечення конфіденційності і цілісності інформації на замовлення;

тання порогів уразливості. Результати визначення повинні бути задокументовані і розглянуті усіма зацікавленими сторонами.

Вимоги з ІБ і засоби управління повинні відображати цінність інформації для бізнесу, яка захищається і потенційний негативний вплив на бізнес, який може бути наслідком недостатньо надійного захисту.

Визначення та управління вимогами з ІБ і відповідними процесами повинні бути об'єднані на ранніх стадіях проектів ІС. Рання увага до вимог з ІБ, наприклад, на стадії проектування, може призводити до більш результативних і економічно ефективних рішень.

Вимоги з ІБ повинні також враховувати:

а) рівень надійності, необхідний для ідентифікаційної інформації користувачів, щоб встановити вимоги до їх автентифікації;

б) процеси забезпечення доступу і авторизації як для звичайних користувачів, так і для привілейованих або технічних фахівців;

в) інформування користувачів і операторів про їх обов'язки та відповідальність;

г) потреби, пов'язані з необхідним захистом використовуваних активів, особливо, які стосуються готовності, конфіденційності та цілісності;

д) вимоги, що випливають з бізнес-процесів, такі як контроль і реєстрація транзакцій, вимоги до незаперечності авторства;

е) вимоги, що встановлюються іншими засобами забезпечення захисту, наприклад, засобами взаємодії з системами реєстрації та моніторингу або виявлення витоку даних.

Для застосунків, які забезпечують сервіси в соціальних мережах або здійснюють транзакції, повинні бути прийняті до уваги спеціальні засоби.

Для придбаних товарів процес тестування і закупівлі повинен бути наступним. Контракти з постачальником повинні містити встановлені вимоги щодо безпеки. У тих випадках, коли функціональність пропонованих продуктів, пов'язана із захистом, не задовольняє встановленим вимогам, повинні бути переглянуті ризики і засоби управління до покупки продукту.

Повинно бути вивчено і виконано наявне керівництво з налаштування захисту продукту, відповідне останньому складу програм/служб системи. Критерії прийняття продуктів повинні бути визначені, наприклад, з точки зору їх функціональності, яка гаран-

Стандарти:

– ISO/IEC 27000 – IT. Методи забезпечення безпеки. СМІБ. Огляд і словник (Information technology. Security techniques. Information security management systems. Overview and vocabulary.) Введення в сімейство стандартів, а також глосарій загальних термінів;

– ISO/IEC 27001 – IT. Методи забезпечення безпеки. СМІБ. Вимоги (Information technology. Security techniques. Information security management systems. Requirements). Стандарт для створення, реалізації, контролю та вдосконалення СМІБ (на основі британського стандарту BS 7799 Частина 2);

– ISO/IEC 27002, BS 7799-1: 2005, BS ISO/IEC 17799: 2005 – IT. Методи забезпечення безпеки. Практичні правила управління ІБ. Кодекс правил СМІБ (Information technology. Security techniques. Code of practice for information security management), (раніше відомої як ISO/IEC 17799 сам заснований на британському стандарт BS 7799 Частина 1, останній раз переглядався в 2005 і перейменований ISO / IEC 27002: 2005 в липні 2007 року);

– ISO/IEC 27003 – IT. Методи забезпечення безпеки. Керівництво по впровадженню СМІБ (Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance);

– ISO/IEC 27004 2009 – IT. Методи забезпечення безпеки. Вимірювання ефективності СМІБ (Information technology. Security techniques. Information security management. Measurement);

– ISO/IEC 27005 – IT. Методи забезпечення безпеки. Управління ризиками ІБ. Призначений для надання допомоги в оцінці ризику при впровадженні СМІБ – управління ризиками (Information technology. Security techniques. Information security risk management). Випущений в червні 2008р. Остання редакція стандарту випущена 19 травня 2011р.;

– ISO/IEC 27006 – IT. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації СМІБ (Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems);

– ISO/IEC 27007 – IT. Методи забезпечення безпеки. Керівництво з проведення аудиту СМІБ (Information technology –

Security techniques – Guidelines for information security management systems auditing);

– ISO/IEC TR 27008 – IT. Методи забезпечення безпеки. Настанови для аудиторів з оцінки органів управління (Information technology – Security techniques – Guidelines for auditors on information security controls);

– ISO/IEC 27010 – IT. Методи забезпечення безпеки. Менеджмент забезпечення ЗІ між секторами і організаціями (Information technology – Security techniques – Information security management for inter–sector and inter–organizational communications);

– ISO/IEC 27011 – IT. Методи забезпечення безпеки. Настанови щодо управління ЗІ організацій, що пропонують телекомунікаційні послуги, на основі ISO / IEC 27002 (Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO / IEC 27002);

– ISO/IEC 27013 – IT. Методи забезпечення безпеки. Керівництво щодо інтегрованого впровадження ISO / IEC 27001 та ISO / IEC 20000-1 (Information technology – Security techniques – Guidance on the integrated implementation of ISO / IEC 27001 and ISO / IEC 20000-1);

– ISO/IEC TR 27015 – IT. Методи забезпечення безпеки. Структура забезпечення захисту. Настанови щодо менеджменту ІБ для фінансових операцій (Information technology – Security techniques – Information security management guidelines for financial services);

– ISO/IEC 27031 – IT. Методи забезпечення безпеки. Керівництво по забезпеченню готовності інформаційних і комунікаційних технологій до їх використання для управління безперервністю бізнесу. (Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity (FDIS));

– ISO/IEC 27032 – IT. Методи забезпечення безпеки. Настанови щодо кібербезпеки (Information technology – Security techniques – Guidelines for cybersecurity);

– ISO/IEC 27033-1 – IT. Методи забезпечення безпеки. Мережева безпека. Частина 1. Огляд та концепції (Information

е) дозволене використання конфіденційної інформації та права підписанта на використання інформації;

ж) права на контроль діяльності, пов'язаної з конфіденційною інформацією;

з) процес повідомлення і звіту про несанкціоноване розголошення або витік конфіденційної інформації;

и) терміни, в які інформація повинна бути повернута або знищена в разі припинення дії угоди;

к) очікувані дії, які повинні бути зроблені в разі порушення угоди.

Залежно від вимог організації до ІБ може знадобитися відобразити в угоді про конфіденційність та нерозголошення і інші аспекти.

Угоди про конфіденційність і нерозголошення повинні відповідати чинному законодавству і нормативним документам в тій юрисдикції, в якій вони застосовуються.

Вимоги до угод про конфіденційність і нерозголошення повинні переглядатися періодично і в тому випадку, коли відбуваються зміни, що зачіпають ці вимоги.

Угоди про конфіденційність і нерозголошення захищають інформацію організації і доводять до відома підписантів їх обов'язки по захисту, використання та розголошення інформації в дусі відповідальності і повноважень. Організації може знадобитися використовувати різні форми угод про конфіденційність і нерозголошення в залежності від обставин [1, 2].

4.10. Впровадження та експлуатація інформаційних систем Вимоги щодо безпеки для ІС

Ціль: гарантувати, що безпека є невід’ємною частиною ІС протягом всього життєвого циклу Це також включає вимоги для ІС, які забезпечують надання послуг з використанням публічних (загальнодоступних) мереж.

1) Аналіз та специфікація вимог ІБ. Вимоги щодо ІБ має бути долучено в положення щодо бізнес-вимог до нових ІС або модернізацій до наявних ІС.

Вимоги з ІБ повинні бути визначені, використовуючи різні методи, такі як виділення вимог щодо відповідності з політиками і регламентами, моделювання загроз, аналіз інцидентів або викорис-

а) відповідний схемі класифікації, прийнятої організацією, захист повідомлень від несанкціонованого доступу, зміни або відмови в обслуговуванні;

б) забезпечення правильної адресації і передачі повідомлення;

в) надійність і доступність послуги;

г) правові аспекти, наприклад, вимоги до електронних підписів;

д) отримання схвалення до використання зовнішніх громадських сервісів, таких як служб миттєвих повідомлень, соціальних мереж або файлообмінників;

е) більш високий рівень автентифікації при контролі доступу із загальнодоступних мереж.

Існує багато видів електронних повідомлень, таких як електронна пошта, обмін електронними даними і соціальні мережі, які відіграють певну роль у бізнес-комунікаціях.

4) Угоди щодо конфіденційності або нерозголошення. Вимоги до угод щодо конфіденційності або нерозголошення, які відображують потреби організації в ЗІ, мають бути ідентифіковані, задокументовані та регулярно переглядатися.

Угоди про конфіденційність або нерозголошення повинні встановлювати вимоги щодо захисту конфіденційної інформації в юридично зобов'язуючій формі. Угоди про конфіденційність або нерозголошення повинні бути застосовані до зовнішніх сторін або працівників організації. Зміст повинен визначатися в залежності від типу сторони, яка приймає зобов'язання, и її прав доступу або обробки конфіденційної інформації. Для визначення вимог до угод про конфіденційність або нерозголошення має бути прийнято до уваги наступне:

а) визначення інформації, що підлягає захисту (наприклад, конфіденційна інформація);

б) очікуваний термін дії угоди, включаючи випадки, коли конфіденційність повинна забезпечуватися протягом невизначеного часу;

в) дії, необхідні при розірванні угоди;

г) обов'язки і дії тих хто підписали угоду для уникнення несанкціонованого розголошення інформації;

д) володіння інформацією, комерційними таємницями і інтелектуальною власністю і як це пов'язано із захистом конфіденційної інформації;

technology – Security techniques – Network security – Part 1: Overview and concepts);

– ISO/IEC 27033-2 – IT. Методи забезпечення безпеки. Захист мережі. Частина 2. Настанови щодо проектування та впровадження захисту мережі (Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security);

– ISO/IEC 27033-3 – IT. Методи забезпечення безпеки. Мережева безпека. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування і питання управління (Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues);

– ISO/IEC 27034-1 – IT. Методи забезпечення безпеки. Безпека застосування. Частина 1. Огляд та поняття (Information technology – Security techniques – Application security – Part 1: Overview and concepts);

– ISO/IEC 27035 – IT. Метод забезпечення безпеки. Управління випадковостями в системі ІБ (Information technology – Security techniques – Information security incident management);

– ISO / IEC 27037 – IT. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних (Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence);

– ISO/IEC WD 27006 – IT – Методи забезпечення безпеки – Вимоги до органів, які проводять аудит і сертифікацію СМІБ (Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems);

– ISO/IEC DIS 27014 – IT – Методи забезпечення безпеки – Керівництво з ІБ (Information technology – Security techniques – Governance of information security);

– ISO/IEC PDTR 27015 – Proposal on an Information security management guidelines for financial and insurance services – Пропозиція з ІБ керуючі управлінські принципи для фінансових і страхових послуг;

– ISO/IEC PDTR 27016 – IT – Методи забезпечення безпеки – Управління ІБ – Організаційна економіка (Information technology – Security techniques – Information security management – Organizational economics);

– ISO/IEC WD 27017 – IT – Методи забезпечення безпеки – Безпеки Cloud computing і системи управління приватного життя – Безпека управління (Information technology – Security techniques – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002);

– ISO/IEC WD 27018 – Code of practice for data protection controls for public cloud computing services;

– ISO/IEC 27036 – IT Security. Security techniques. Guidelines for security of outsourcing (DRAFT) – Керівництво з аутсорсингу безпеки;

– ISO/IEC 27033-4 – Забезпечення безпеки міжмережевих взаємодій за допомогою шлюзів безпеки – загрози, методи проектування та механізми контролю (Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways);

– ISO/IEC 27033-5 – IT. Методи забезпечення безпеки. Забезпечення безпеки Віртуальних Приватних Мереж – загрози, методи проектування та механізми контролю (Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Network (VPNs));

– ISO/IEC 27033-6 – Information technology – Security techniques – Network security – Part 6: Securing IP network access using wireless – Конвергенція в IP мережах (Визначення загроз, методів проектування і механізмів контролю в IP мережах з конвергенцією даних);

– ISO/IEC 27034-2 – Organization Normative Framework (draft) – Нормативна база організації;

– ISO/IEC 27034-3 – Application Security Management Process (pre–draft) – Процес управління безпекою додатків;

– ISO/IEC 27034-4 – Application security validation (pre–draft) – Оцінка безпеки додатків;

2) Угоди щодо обміну інформацією. Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо безпечного обміну бізнес-інформацією.

Угоди про передачу інформації повинні включати наступне:

а) обов'язки керівництва з контролю і повідомленню про передачу, відправлення та одержання;

б) процедури для забезпечення простежуваності і незаперечності авторства;

в) мінімальні технічні стандарти для пакетування і передачі;

г) угоди про умовне депонування;

д) стандарти з ідентифікації кур'єрів;

е) відповідальність і зобов'язання у разі інцидентів ІБ, таких як втрата даних;

ж) використання узгодженої системи маркування уразливої і критично важливої інформації, яка гарантує, що зміст маркування зрозумілий відразу і що інформація належним чином захищена;

з) технічні стандарти для запису і читання інформації та ПЗ;

и) будь-які спеціальні заходи захисту, які потрібні для захисту уразливих елементів, такі як криптографія;

к) ланцюжок відповідальності і збереження інформації в процесі передачі;

л) прийнятні рівні контролю доступу.

Повинні бути розроблені і підтримуватися політики, процедури та стандарти щодо ЗІ та фізичних носіїв в процесі передачі, а також вони повинні бути вказані в угодах про передачу.

Частина будь-якої угоди, присвячена ІБ, повинна відображати ступінь конфіденційності бізнес-інформації, яка бере участь в передачі.

Угоди можуть бути в електронному вигляді або рукописному, або ж мати форму офіційного договору. Відносно конфіденційної інформації конкретні механізми, використовувані для передачі такої інформації, повинні бути єдиними для всіх організацій і типів угод.

3) Електронний обмін повідомленнями. Інформація, яка міститься в електронних повідомленнях, має бути захищена належним чином.

Рекомендації з ІБ електронних повідомлень повинні включати наступне:

національному та місцевому законодавству і нормативним документам;

з) засоби управління і обмеження, пов'язані з використанням комунікаційних пристроїв, наприклад, автоматичне перенаправлення електронної пошти на зовнішні адреси;

и) рекомендації персоналу вживати заходів обережності, щоб не розкрити конфіденційну інформацію;

к) не залишати повідомлення, що містять конфіденційну інформацію на автовідповідачах, тому що вони можуть бути прослухані неавторизованими особами, збережені в системах загального користування або записані на іншому пристрої в результаті помилкового набору номера;

л) інформування персоналу про проблеми, пов'язані з використанням факсів та відповідних послуг, а саме:

1) неавторизованого доступу до записів повідомлень і їх прослуховуванням;

2) навмисного або випадкового програмуванням факсу на відправку повідомлень на певні номери;

3) відсилання документів і повідомлень на невірний номер або в результаті помилкового набору чи виклику збереженого неправильного номеру.

Крім того, персонал повинен пам'ятати, що не слід вести конфіденційні розмови в громадських місцях або по небезпечним каналах зв'язку, у відкритих офісах і кімнатах для переговорів.

Послуги з передачі інформації повинні відповідати всім законодавчим вимогам.

Передача інформації може здійснюватися за допомогою використання ряду різних засобів зв'язку, включаючи електронну пошту, голосовий та факсимільний зв'язок, а також відео. Передача програм може здійснюватися за допомогою різних носіїв, включаючи завантаження з Інтернету і отримання від постачальника, що продає готові продукти.

Повинні бути враховані юридичні наслідки, вплив на бізнес і безпеку, пов'язані з обміном електронними даними, електронною торгівлею і електронними комунікаціями, а також вимогами до засобів управління.

– ISO/IEC 27034-5 – Protocols and application security control data structure (pre-draft) – Протоколи і структура керуючої інформації для забезпечення безпеки додатків (XML схема);

– ISO/IEC 27034-6 – Security guidance for specific applications (pre-draft) – Керівництво по забезпеченню безпеки конкретних програм;

– ISO/IEC WD 27035-1 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 1: Принципи управління інцидентами (Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management);

– ISO/IEC WD 27035-2 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 2: Керівні принципи щодо реагування на інциденти (Information technology – Security techniques – Information security incident management – Part 2: Guidelines for incident response readiness) ;

– ISO/IEC WD 27035-3 – IT. Методи забезпечення безпеки – ІБ управління інцидентами – Частина 3: Керівництво по CSIRT операціям (Information technology – Security techniques – Information security incident management – Part 3: Guidelines for CSIRT operations);

– ISO/IEC DIS 27036-1 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 1: Огляд та концепції (Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts);

– ISO/IEC DIS 27036-2 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 2: Загальні вимоги (Information technology – Security techniques – Information security for supplier relationships – Part 2: Common requirements);

– ISO/IEC DIS 27036-3 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 3: Посібник з безпеки ІКТ ланцюжка поставок (Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for ICT supply chain security);

– ISO/IEC WD 27036-4 – IT. Методи забезпечення безпеки – ІБ для відносин з постачальниками – Частина 4: Посібник з безпеки аутсорсингу (Information technology – Security techniques –

Information security for supplier relationships – Part 4: Guidelines for security of outsourcing);

– ISO/IEC DIS 27038 – Information technology – Security techniques – Specification for Digital Redaction;

– ISO/IEC CD 27039 – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems;

– ISO/IEC CD 27040 – Information technology – Security techniques – Storage security;

– ISO/IEC CD 27042 – Guidelines for the analysis and interpretation of digital evidence;

– ISO/IEC CD 27043 – Investigation principles and processes;

– ISO/IEC WD 27044 – Security Information and Event Management (SIEM) та ін.

Питання для самоконтролю

1) Чим менеджер відрізняється від підприємця?
2) Що є предметом менеджменту?
3) Які ви знаєте основні функції менеджменту?
4) Назвіть загальні принципи управлінської діяльності.
5) Якій найсуттєвіший внесок в менеджмент зроби А. Файоль?
6) Що є предметом сучасного менеджменту?
7) Розкрийте сутність понять конфіденційність, цілісність та доступність?
8) Що таке актив?
9) Розкрийте сутність поняття системи менеджменту інформаційної безпеки?
10) Наведіть приклад складних і простих активів?
11) Що таке цикл PDCA?
12) Які міжнародні організації беруть участь у забезпечені та підтримки інформаційної безпеки?
13) Що регламентує стандарт ISO/IEC 27001 та ISO/IEC 27002?

Автентифікації, шифрування і технологій контролю доступу на рівні користувача сучасних бездротових мереж, заснованих на стандартах, може бути досить для прямого з'єднання до внутрішньої мережі організації при належному виконанні.

Мережі часто виходять за межі організації, оскільки ділове співробітництво вимагає взаємодії і спільного використання мережевого обладнання і пристроїв обробки інформації. Таке розширення може збільшувати ризик несанкціонованого доступу до ІС організації, що використовують мережу, деякі з яких вимагають захисту від користувачів інших мереж в силу їх критичної важливості або уразливості.

Обмін інформацією

Ціль: Підтримувати безпеку інформації, якою обмінюються всередині організації та з зовнішнім об’єктом.

1) Політики та процедури обміну інформацією. Мають бути наявними офіційно оформлені політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів засобів комунікації.

Процедури і засоби управління, яким необхідно слідувати при використанні комунікаційного обладнання для передачі інформації, повинні передбачати наступне:

а) процедури, призначені для ЗІ, що передається від перехоплення, копіювання, зміни, перенаправлення і руйнування;

б) процедури для виявлення шкідливого коду, який може передаватися засобами електронного зв'язку, і захисту від нього;

в) процедури для захисту конфіденційної інформації в електронному вигляді, що передається в формі застосунку;

г) політику або керівні вказівки, що визначають допустиме застосування комунікаційних пристроїв;

д) обов'язки персоналу, зовнішніх сторін і будь-яких інших користувачів не спричиняти дії, що компрометують організацію, наприклад, за допомогою наклепів, образ, неправомірного уявлення себе від імені організації, розсилки листів по ланцюжку, неавторизованих закупівель і т. д.;

е) використання криптографічних засобів, наприклад, для захисту конфіденційності, цілісності та достовірності інформації;

ж) рекомендації щодо термінів зберігання та утилізації всієї ділової переписки, включаючи повідомлення, що відповідають

Особливостями в забезпеченні безпеки мережевих послуг можуть бути:

а) сукупність методів, що застосовуються для захисту мережевих послуг, таких як автентифікація, шифрування і керувати з'єднаннями з мережею;

б) технічні параметри, необхідні для захищених з'єднань з наданими за послугою мережами відповідно до правил мережевих з'єднань;

в) процедури використання мережевих послуг з метою обмеження доступу до надаваних мереж або застосунків, якщо необхідно.

3) Сегментація в мережах. У мережі мають бути сегментовані групи інформаційних послуг, користувачів, а також ІС.

Один з методів управління великими мережами полягає в поділі їх на окремі мережеві домени.

Домени можуть бути виділені за рівнем довіри (наприклад, домен загального доступу, домен робочих станцій, домен сервера), по підрозділах (наприклад, відділ кадрів, фінансовий, маркетингу) або за сукупністю ознак (наприклад, домен сервера, з'єднаний з множиною структурних підрозділів). Поділ може бути здійснено або фізичним поділом на різні мережі, або логічним (наприклад, віртуальні приватні мережі, VPN).

Межі кожного домена повинні бути чітко визначені. Обмін між доменами дозволений, але повинен бути контрольованим на кордоні з використанням шлюзів (наприклад, брандмауерів, фільтруючих маршрутизаторів). Критерії розподілу мереж на домени і дозволу доступу через шлюзи повинні базуватися на оцінці вимог з безпеки кожного домена. Оцінка повинна проводитися відповідно до політики контролю доступу, вимог до доступу, значущості та категорії оброблюваної інформації, а також з урахуванням відносної вартості та впливу застосовуваних технологій шлюзів на продуктивність.

Бездротові мережі вимагають спеціальних рішень в силу того, що в них складно визначити межі. Відносно критично важливих сегментів слід прийняти підхід, при якому всі запити з бездротових мереж розглядаються як зовнішні і відрізняються від запитів внутрішніх мереж до тих пір, поки запит не пройде шлюз і не буде дозволений доступ до внутрішніх систем відповідно до політики мережевого контролю.

СПИСОК ЛІТЕРАТУРИ ДО ПЕРШОГО РОЗДІЛУ

1) Й.С. Завадський, Менеджмент: «Management», 2-е. вид., К.,Українсько-фінський інститут менеджменту і бізнесу, 1998.

2) Г. Я. Гольдштейн, Основы менеджмента: Конспект лекций. Таганрог: ТРТУ, 1997, Издание второе дополненное.

3) Д.В. Овсянко, «Классики теории менеджмента». Вестник Санкт-Петербургского университета, Сер 8, Вып. 2. (№16) 2004.

4) Дж.М. Кейнс, Общая теория занятости, процента и денег, М.: Прогресс, 1978.

5) В.Автономова, О.Ананьина, Н. Макашевой, История экономических учений: учебное пособие, М.: ИНФРА-М, 2004.

6) Е.Ф. Прокушев, Менеджмент первичного уровня., М.: Издательский Дом «Дашков и К», 1999.

7) А.А. Дмитриев: «ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях», «Das Management» №1, 2009, с. 36-39;

8) «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

9) «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общие сведения и словарь» ISO/IEC 27000:2014, ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия), 2014, с. 41.

10) В.О. Лебединець, С.М. Коваленко, Н.О. Тахтаулова, «Імплементація циклу Демінга-Шухарта (PDCA) при регламентації процесів системи управління якістю фармацевтичного підприємства», Управління правління, економіка та забезпечення якості в фармації, № 1(21), с. 11-17, 2012.

11) Деятельность международных организаций в сфере информационной безопасности [Електронний ресурс], НОУ «ИНТУИТ», 2019., Режим доступу: https://www.intuit.ru/ studies/courses/ 563/419/lecture/9570?page=2 (10 січня 2019).

12) Деятельность специализированных международных организаций и объединений в сфере информационной безопасности, [Електронний ресурс], НОУ «ИНТУИТ», 2019., Режим доступу:

https://www.intuit.ru/ studies/ courses/563/419/lecture/9571 (10 січня 2019).

13) О.О. Цвілій, Безпека інформаційних технологій: сучасний стан стандартів ISO27K системи управління інформаційною безпекою, *Телекомунікаційні та інформаційні технології*., №2, с. 73-79, 2014.

в) повинні бути зроблені спеціальні заходи для захисту конфіденційності та цілісності даних, переданих по мережах загального користування або бездротових мереж, а також підключених систем і застосунків. Спеціальні заходи можуть також знадобитися для підтримки готовності мережевих сервісів і підключених комп'ютерів;

г) повинна вестися відповідна реєстрація та контроль з метою фіксації і виявлення дій, які можуть вплинути на ІБ або є важливими для неї;

д) дії з управління повинні тісно координуватися як для того, щоб оптимізувати обслуговування організації, так і для гарантії того, що засоби управління застосовуються узгоджено в рамках інфраструктури обробки інформації;

е) системи в мережах повинні проходити процедуру автентифікації;

ж) системні з'єднання в мережі повинні бути обмежені.

Додаткова інформація з мережевої безпеки може бути знайдена в стандарті ISO / IEC 27033.

2) Безпека послуг мережі. Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами мережі має бути ідентифіковано і міститися в будь-якій угоді щодо послуг мережі як для послуг, які надає сама організація, так і для аутсорсингових послуг.

Повинна бути визначена і регулярно перевірятися здатність провайдера мережевих послуг управляти узгодженням послуги, забезпечуючи безпеку, а також має бути погоджено право на аудит.

Повинні бути визначені заходи щодо забезпечення безпеки, необхідні для тієї чи іншої послуги, такі як засоби безпеки, рівень обслуговування і вимоги до управління. Організація повинна гарантувати, що провайдери мережевих послуг здійснюють ці заходи.

Мережеві послуги включають в себе забезпечення підключення, послуги приватних мереж (VPN), мереж з розширеними можливостями (VAN), а також рішення з мережевої безпеки з можливістю управління, такі як брандмауери і системи виявлення вторгнень. Ці послуги можуть варіюватися в діапазоні від простого надання смуги пропускання до складних пропозицій, що розширюють можливості.

Заходи безпеки аудиту ІС. Вимоги аудиту та діяльність, що охоплює перевірки систем, які перебувають в експлуатації, має бути ретельно сплановано та погоджено, щоб мінімізувати ризик порушення бізнес-процесів.

Необхідно мати на увазі наступні рекомендації:

а) при аудиті вимоги щодо доступу до систем і даних повинні бути узгоджені з відповідним керівництвом;

б) сферу застосування тестів технічного аудиту повинна бути узгоджена і контролюватися;

в) перевірочні тести повинні бути обмежені доступом до ПЗ та даних тільки на читання;

г) доступ, відмінний від режиму тільки на читання, повинен бути дозволений тільки для ізольованих копій системних файлів, які повинні бути видалені після завершення аудиту або відповідним чином захищені, якщо є зобов'язання зберігати їх в силу вимог щодо документування аудиту;

д) вимоги до спеціальної або додаткової обробки повинні бути встановлені і узгоджені;

е) перевірочні тести, які можуть впливати на можливості системи, повинні запускатися у неробочій час;

ж) будь-який доступ повинен контролюватися і реєструватися для забезпечення можливості простеження [1, 2].

4.9. Безпека комунікацій

Управління безпекою мережі

Ціль: Забезпечити захист інформації в мережах та захист засобів оброблення інформації, що їх підтримує.

1) Заходи безпеки мережі. Треба відповідним чином управляти й захищати мережі для ЗІ в системах і прикладних програмах.

Повинні бути впроваджені засоби управління для гарантії БІ в мережах і захисту підключених сервісів від несанкціонованого доступу. Зокрема, слід взяти до уваги наступне:

а) повинні бути встановлені обов'язки і процедури для управління мережевим обладнанням;

б) там, де це може бути застосовано, відповідальність, пов'язана з експлуатацією мереж, повинна бути відділена від експлуатації комп'ютерів;

Розділ 2. СКЛАДОВІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Переваги впровадження СМІБ

Прийняття необхідності СМІБ є стратегічним рішенням для організації. На встановлення та впровадження СМІБ організації впливають такі фактори як потреби та цілі організації, вимоги щодо її безпеки, організаційні процеси, що застосовуються, а також розмір та структура організації. Але очікується, що всі ці впливові фактори зміняться з часом. Крім того, СМІБ забезпечує збереження конфіденційності, цілісності та доступності інформації, застосовуючи процес управління ризиками тим самим запевняючи зацікавлені сторони, що ризики належним чином контролюються.

Важливо те, що СМІБ є частиною інтегрованих процесів організації та загальної структури управління, а отже питання забезпечення ІБ розглядаються під час розроблення процесів, ІС та контролю. Очікується, що реалізація СМІБ буде змінюватися відповідно до потреб організації.

Перевагами впровадження СМІБ можуть бути:

1) Зрозумілість інформаційних активів для менеджменту компанії.

Організація повинна управляти активами:

– інвентаризація активів;

– визначення відповідальних за активи;

– розробка принципів класифікації активів за їхньою важливістю, правовими вимогами і критичністю для організації;

– ідентифікація активів відповідно до принципів класифікації.

2) Результативне виконання політики безпеки (ПБ) (виявляти і виправляти слабкі місця в системі ІБ).

Керівництво повинно:

– розробляти політику СМІБ;

– встановлювати цілі і плани;

– розподіляти відповідальність в області ІБ;

– повідомляти всіх співробітників;

– забезпечувати ресурсами;

– приймати рішення про прийнятні рівні ризиків;

– забезпечувати проведення внутрішніх аудитів;

– проводити аналіз СМІБ.

3) Регулярне виявлення загроз і уразливостей безпеки для існуючих бізнес-процесів.

Організація повинна ідентифікувати ризики:

– ідентифікувати активи;

– ідентифікувати загрози цим активам;

– ідентифікувати уразливості, які можуть бути використані цими загрозами;

– визначити вплив, який може призвести до втрати конфіденційності, цілісності і доступності ресурсів.

4) Розрахунок ризиків і прийняття рішень на основі бізнес-цілей.

Організація повинна проаналізувати та оцінити ризики:

– оцінити збиток бізнесу;

– оцінити ймовірність виникнення порушення;

– оцінити рівні ризиків;

– визначити, чи є ризик прийнятним, чи потрібна обробка ризику з використанням критеріїв прийняття ризику.

5) Ефективне управління підприємством в критичних ситуаціях.

Організація повинна управляти безперервністю бізнесу:

– визначити і впровадити процеси для безперервності бізнесу;

– ідентифікувати події, які можуть призвести до порушень бізнес-процесів;

– визначити можливості та ступені впливу;

– розробити плани відновлення;

– визначити пріоритети планів для їх тестування і підтримки;

– тестувати і регулярно оновлювати плани.

6) Демонстрація прозорості і чистоти бізнесу перед законом завдяки відповідності до стандарту.

Організація повинна:

– визначити законодавство, що використовуватиметься;

– забезпечити захист інтелектуальної власності;

– забезпечити захист записів від втрати, руйнування і фальсифікації відповідно до вимог законодавства;

– забезпечити захист персональних даних і приватної інформації;

м) визначити процедури обробки ситуації, коли уразливість вже виявлена, але немає відповідних контрзаходів. У такій ситуації організації повинна оцінити ризики, пов'язані з відомою уразливістю і визначити відповідні дії з виявлення та коригувальні дії.

Управління технічними уразливостями може розглядатися як під функція управління змінами і, таким чином, може використовувати процеси та процедури управління змінами.

Виробники часто знаходяться під значним тиском необхідності випустити патчі якомога швидше. Внаслідок чого існує можливість того, що патч не усуває проблему належним чином і має негативні побічні ефекти. Також в деяких випадках деінсталяція патча після його застосування не може бути виконана досить легко.

Якщо відповідне тестування патча неможливо, наприклад, в силу високої вартості або нестачі ресурсів, то може бути розглянута можливість затримки його застосування для оцінки відповідних ризиків, заснованої на звітах щодо застосування патча іншими користувачами. Може бути корисно використання стандарту ISO / IEC 27031.

2) Обмеження на інсталяцію ПЗ. Має бути розроблено та впроваджено правила стосовно інсталяції ПЗ користувачами.

Організація повинна визначити і слідувати жорсткій політиці, яка визначає, яке ПЗ користувачі можуть встановлювати.

Необхідно виходити з принципу мінімальних привілеїв. Користувачі можуть мати можливість установки ПЗ, якщо тільки їм дано такі повноваження. Організація повинна визначити, якого роду установки дозволені (наприклад, оновлення або патчі з безпеки існуючого ПЗ), а також які види установок заборонені (наприклад, програми для особистого користування або програми, походження яких, з урахуванням потенційної шкодо чинності, невідомо чи підозріло). Розглянуті повноваження повинні даватися з урахуванням ролі користувача.

Неконтрольовані установки ПЗ на комп'ютерах можуть вести до появи уразливостей і, тим самим, до витоку інформації, втрати цілісності або інших інцидентах ІБ, або до порушення авторських прав.

Розгляд аудиту інформаційних систем

Ціль: Мінімізувати вплив аудиту на системи, які перебувають у промисловій експлуатації.

римки поінформованості про них. Ці інформаційні ресурси повинні оновлюватися відповідно до змін в реєстрі або коли виявляються інші нові або корисні ресурси;

в) повинен бути визначений термін реагування на повідомлення про можливі істотні технічні уразливості;

г) як тільки виявлена технічна уразливість, організація повинна визначити пов'язані з нею ризики і необхідні дії. Такого роду дії можуть включати в себе випуск патчів для усунення уразливостей в системі або застосування інших заходів;

д) в залежності від терміновості усунення технічної уразливості, дії повинні вживатися або відповідно до процедур управління змінами, або відповідно до процедур обробки інцидентів ІБ;

е) якщо патч доступний на легальному джерелі, то повинні бути оцінені ризики, пов'язані з установкою патча (ризики, викликані уразливістю, необхідно порівняти з ризиками установки патча);

ж) патчі повинні бути протестовані та оцінені до їх установки для гарантії того, що вони результативні і не призводять до неприпустимих побічних ефектів, якщо немає доступного патча, необхідно розглянути можливість застосування інших заходів, таких як:

1) припинення користування сервісами та інструментами, пов'язаними з уразливостями;

2) настройка або додавання засобів контролю доступу, наприклад, брандмауерів, на стику мереж;

3) посилення моніторингу для виявлення реальних атак;

4) додаткове інформування про уразливості;

з) для всіх вжитих заходів повинні зберігатися контрольні журнали;

и) процес управління технічними уразливостями повинен регулярно контролюватися і оцінюватися з тим, щоб гарантувати його результативність і ефективність;

к) системи з високим рівнем ризику повинні розглядатися в першу чергу;

л) результативний процес управління технічними уразливостями повинен бути пов'язаний з діяльністю з управління інцидентами, щоб передавати дані про уразливість службі обробки інцидентів і забезпечувати технічними процедурами, які повинні бути виконані, якщо станеться інцидент;

– запобігти нецільовому використанню засобів обробки інформації користувачем.

7) Захист від рейдерських атак на ранніх стадіях

Рейдери – фахівці з перехоплення оперативного управління або власності фірми за допомогою спеціально ініційованого бізнес-конфлікту. **Рейдерство** – виведення активів з володіння законних власників. Одна з можливих схем роботи рейдера – створити підприємству максимальну кількість проблем, а потім забрати у власників і менеджменту за безцінь з тим, щоб з тисячократним прибутком продати підприємство або його майно третім сторонам.

Уразливості підприємства породжують рейдерське захоплення. Рідко підприємства не мають «гріхів». Ці гріхи, а точніше компрометуюча інформація знаходиться в рамках загальної ІС підприємства. Приховавши цю інформацію від третіх осіб можна уникнути ініціювання рейдерського захоплення.

Сам процес рейдерського захоплення базується на вивченні внутрішніх процесів підприємства, правил і норм його роботи.

Ця інформація дозволяє чітко спланувати і провести рейдерське захоплення в найбільш підходящий момент часу. Закриття цієї інформації або дезінформування рейдерів не дозволить здійснити план із захоплення підприємства.

8) Зниження і оптимізація вартості підтримки системи безпеки (див. рис. 2.1).

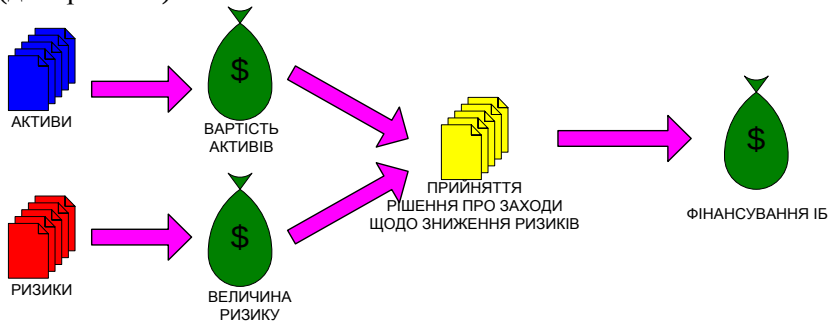


Рис. 2.1. Зниження і оптимізація вартості підтримки системи безпеки

9) Інтеграція підсистеми ІБ в загальну систему менеджменту (див. рис. 2.2).

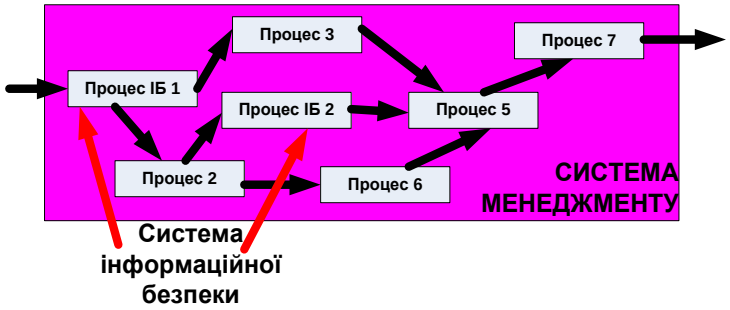


Рис. 2.2. Інтеграція підсистеми ІБ в загальну систему менеджменту

10) Демонстрація клієнтам, партнерам, власникам бізнесу своєї прихильності до ІБ.

11) Міжнародне визнання і підвищення авторитету компанії, як на внутрішньому, так і на зовнішніх ринках [1, 2].

2.2. Сфери дії СМІБ

Місце СМІБ в організації

Великі підприємства гірничо-металургійного комплексу, машинобудівні і хімічні можуть мати СМІБ такого виду:

– СМІБ практично повністю міститься всередині загальної системи менеджменту, тому що основними характеристиками забезпечення безпеки інформації в цьому випадку є цілісність і доступність (див. рис. 2.3).

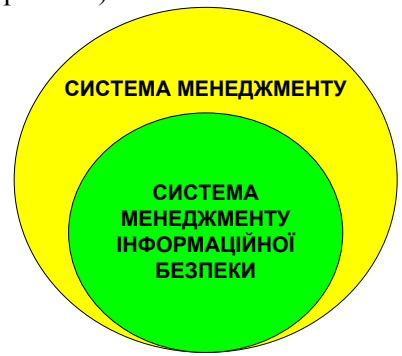


Рис. 2.3. Приклад місця СМІБ у загальній системі менеджменту великого підприємства гірничо-металургійного комплексу

ку застарілих версій. Організація повинна брати до уваги ризики, пов'язані з цією обставиною.

Будь-яке рішення про оновлення до нової версії має ґрунтуватися на вимогах змін, що виходять від бізнесу, і захищеності нової версії, наприклад, введення нової функціональності, пов'язаної з ІБ, або кількості і серйозності проблем ІБ, що впливають на цю версію. Патчі до ПЗ повинні встановлюватися в тих випадках, коли вони можуть допомогти усунути або зменшити уразливість ІБ.

Будь-який вид доступу постачальникам з метою забезпечення підтримки повинен даватися тільки тоді, коли це необхідно, і з дозволу керівництва. Дії постачальників повинні контролюватися.

Комп'ютерне ПЗ може залежати від програм і модулів, що поставляються ззовні, які повинні контролюватися, щоб уникнути неавторизованих змін, здатних породити уразливості в захисті.

Управління технічною уразливістю

Ціль Запобігати використанню технічних уразливостей.

1) Управління технічною уразливістю. Треба отримувати своєчасну інформацію щодо технічних уразливостей ІС, які використовують, оцінювати підвладність організації таким уразливостям і вживати належних заходів, щоб урахувати пов’язаний з цим ризик.

Ведення актуального і повного обліку активів – це необхідна умова для результативного управління технічними уразливостями. Інформація, необхідна для підтримки управління технічними уразливостями, включає в себе найменування постачальника ПЗ, номер версії, поточний стан (наприклад, яке ПЗ встановлено на якій системі) і осіб, відповідальних в організації за це ПЗ.

Повинні вживатися відповідні і своєчасні дії у разі виявлення потенційних технічних уразливостей. Необхідно виконувати наступні рекомендації для розробки результативного процесу управління технічними уразливостями:

а) організація повинна визначити і встановити посади і обов'язки, пов'язані з управлінням технічними уразливостями, включаючи моніторинг, оцінку ризиків, виправлення, відстеження активів і будь-які необхідні обов'язки з координації;

б) для ПЗ та інших технічних систем (включених до реєстру активів) повинні бути визначені інформаційні ресурси, які будуть використані для виявлення істотних технічних уразливостей і підт-

синхронізації всіх серверів з еталонним часом може бути використаний мережевий протокол синхронізації часу (NTP).

Контроль ПЗ, що перебуває в експлуатації

Ціль: Гарантувати цілісність систем, що перебувають в експлуатації.

Інсталяція ПЗ в системах, що перебувають в експлуатації. Мають бути наявними процедури контролю інсталяції ПЗ в системах, що перебувають в експлуатації.

Повинні бути прийняті до уваги наступні рекомендації по контролю змін ПЗ в експлуатованих системах:

а) оновлення експлуатованого ПЗ, додатків і програмних бібліотек повинно виконуватися тільки навченими адміністраторами при наявності відповідного дозволу керівництва;

б) експлуатовані системи повинні містити тільки схвалений виконаний код, але не оцінний код або компілятори,

в) програм та ПЗ ОС повинні встановлюватися тільки після проведення ретельного та успішного тестування. Тести повинні охоплювати такі області, як зручність застосування, безпеку, вплив на інші системи, дружність інтерфейсу і повинні виконуватися на окремих системах, при цьому має бути гарантовано, що всі відповідні вихідні програмні бібліотеки були оновлені;

г) повинна застосовуватися система управління конфігураціями і системне документування для збереження контролю над всім ПЗ, що встановлюється;

д) повинна бути розроблена стратегія відкату до того, як зміни будуть впроваджені;

е) повинен вестися контрольний журнал всіх оновлень робочих програмних бібліотек;

ж) повинні зберігатися попередні версії додатків як міра страховки;

з) застарілі версії ПЗ повинні архівувати разом з необхідною інформацією та змінними, процедурами, параметрами конфігурації і допоміжними програмами і зберігатися в архіві той же термін, що і дані.

Обладнання, що поставляється з ПЗ, яке використовується в експлуатованих системах, має бути забезпечено підтримкою на рівні виробника. Через деякий час продавці ПЗ припинять підтрим-

Конфіденційність (захист від витоків інформації, компрометація даних) також присутня у відносинах з конкурентами, постачальниками і споживачами. Але ступінь важливості цього аспекту в цьому випадку не можна порівняти з внутрішніми інформаційними загрозами.

Для підприємств фінансової сфери, телекомунікаційних послуг, авіакомпаній, державних органів законодавчої і виконавчої влади, управлінь статистики, МВС, СБУ структура може бути такою (див. рис. 2.4):

– СМІБ є однією з основ життєдіяльності організації.

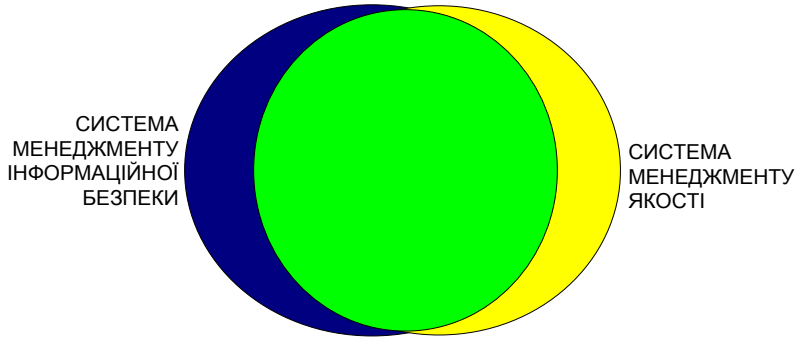


Рис. 2.4. Приклад інтеграція СМІБ з системою менеджменту якості підприємств фінансової сфери

На перше місце за важливістю виходить базова характеристика безпеки інформації – конфіденційність.

Вимоги до конфіденційності вимагають глибокого опрацювання загроз і реалізації заходів захисту.

Для підприємств і організацій середнього розміру СМІБ може мати наступний вигляд:

– неможливо точно визначити місце СМІБ в організації залежно від належності до галузі і її розмірів. Кожне підприємство завжди було й буде унікальним механізмом, зі своїм стилем менеджменту, своїми технологічними та інформаційними механізмами (див. рис. 2.5).

Сфера поширення СМІБ

Чіткий опис меж дії СМІБ.

Сфера дії СМІБ повинна виходити з основної діяльності підприємства.

Рис. 2.5. Приклад інтеграція СМІБ з системами менеджменту підприємств і організацій середнього розміру

Для визначення області дії СМІБ може знадобитися:

– перелік і опис продуктів / послуг підприємства;
– організаційна структура підприємства;
– територіальна структура підприємства.

Приклад: Підприємство – страхова компанія «XYZ» (рис. 2.6)

Продукти:

– страхування фіз. осіб від нещасних випадків;
– страхування юр. осіб (страхування бізнесу);
– страхування вантажів (при перевезеннях);
– аналіз результатів фінансово-господарської діяльності підприємства.

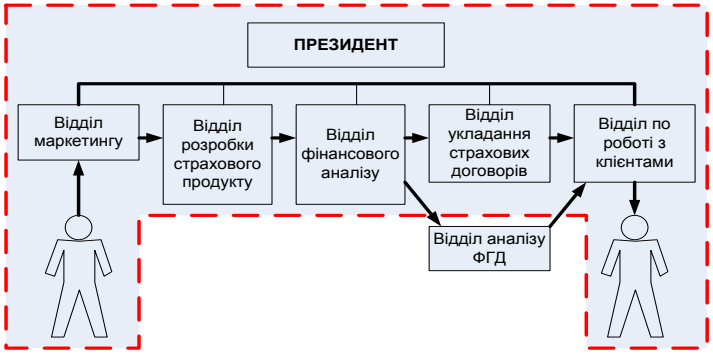


Рис. 2.6. Оргструктура

ту для контрольного зчитування і видалення зайвих записів з файлу.

Системні журнали повинні бути захищені, тому, якщо буде можливість змінювати або видаляти в них дані, то наявність таких змінених журналів може створювати помилкове відчуття безпеки. Для захисту журналів може застосовуватися їх копіювання в режимі реального часу в систему, що знаходиться поза контролем системного адміністратора або оператора.

3) Журнали реєстрації адміністратора та оператора. Діяльність системного адміністратора та системного оператора має реєструватися і журнали аудиту мають бути захищені та регулярно переглядатися.

Користувачі, що володіють привілейованими обліковими записами, можуть мати можливість маніпулювати журналами пристроїв обробки інформації, що знаходяться під їх безпосереднім керівництвом, отже, необхідно захистити і переглядати журнали для забезпечення контролю за привілейованими користувачами.

Для контролю втручань системних і мережевих адміністраторів може застосовуватися система виявлення вторгнень, яка знаходиться поза контролем системних і мережевих адміністраторів.

4) Синхронізація годинників. Годинники всіх важливих систем оброблення інформації в організації або домені безпеки має бути синхронізовано з джерелом часу погодженої точності.

Повинні бути задокументовані внутрішні і зовнішні вимоги до подання часу, синхронності і точності. Такі вимоги можуть бути законодавчими, нормативними, контрактними вимогами, стандартами відповідності або вимогами для внутрішнього моніторингу. Повинен бути визначений стандартний еталон часу для застосування в організації.

Правильна установка комп'ютерних годин є важливою для забезпечення точності контрольних записів, які можуть знадобитися в ході розслідування або як свідчення в рамках судового або дисциплінарного розгляду. Неточні контрольні записи можуть ускладнювати такі розслідування і підривати довіру до подібного роду свідченнями. В якості еталонного часу в системах реєстрації можуть бути використані сигнали точного часу, що передаються по радіо і синхронізовані з національним атомним еталоном часу. Для

е) записи успішних та відхилених системою спроб доступу до даних і інших ресурсів;

ж) зміни в системній конфігурації;

з) використання привілеїв;

и) використання системних утиліт і додатків;

к) файли, до яких отримувався доступ і вид доступу;

л) мережеві адреси і протоколи;

м) попередження, видані системою контролю доступу;

н) активація або вимкнення систем захисту, таких як антивіруси і системи виявлення вторгнень;

о) записи транзакцій, виконаних користувачем у застосунках.

Реєстрація подій служить джерелом даних для автоматизованих систем моніторингу, які здатні генерувати консолідовані звіти і попередження системи безпеки.

Журнали можуть містити важливі дані і персональну інформацію. Повинні бути вжиті відповідні заходи захисту конфіденційності.

Там, де це можливо, системні адміністратори не повинні мати дозволи для стирання або відключення запису їх власних дій.

2) Захист інформації журналів реєстрації. Засоби реєстрування та інформація реєстрації має бути захищено від фальсифікації та несанкціонованого доступу.

Заходи захисту повинні бути націлені на запобігання неавторизованих змін інформації в журналах і проблем функціонування пристроїв ведення журналів, включаючи:

а) зміна типів повідомлень, які були записані;

б) видалення або редагування лог-файлів;

в) нестача необхідного вільного об'єму для запису на носії, що приводить або до збою в запису події, або перезапису інформації про попередні події.

Може знадобитися зберігати в архіві деякі контрольні журнали в рамках політики збереження записів або в силу наявності вимоги збирати і зберігати свідоцтва.

Системні журнали часто містять великий обсяг інформації, значна частина якої не пов'язана з моніторингом ІБ. Для виявлення значимих з точки зору моніторингу ІБ події необхідно передбачити або копіювання записів відповідного типу в інший журнал, або використання відповідних системних утиліт або інструментів ауди-

Сфера поширення СМІБ:

– Проектування страхових продуктів, надання страхових послуг фізичним та юридичним особам [1, 2].

2.3. Інтеграція СМІБ та системи менеджменту якості

Описані процеси СМІБ і їх взаємозв'язок дозволить точно визначити:

– найважливіші активи;

– рух інформаційних потоків і на цій основі визначити загрози та уразливості.

Існуюча документована система менеджменту якості (СМЯ) дозволить:

– скоротити час на розробку основних документів СМІБ;

– побудувати рух документообігу СМІБ за існуючими схемами.

Приклад опису процесу див. рис. 2.7.

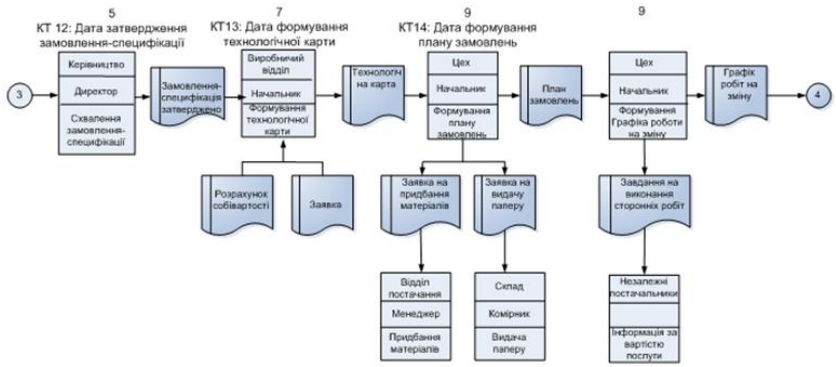


Рис. 2.7. Приклад опису процесу

Принципи управління якістю:

1. Орієнтація на споживача.
2. Лідерство.
3. Залучення персоналу.
4. Процесний підхід.
5. Системний підхід до управління.
6. Постійне поліпшення.
7. Прийняття рішень на підставі фактів.

8. Взаємовигідні відносини з постачальниками.

Стандарт ISO 27001 гармонізований із стандартом на системи менеджменту якості ISO 9001 і ґрунтується на його основних принципах.

Структура документації на вимогу ISO 27001 може бути аналогічна структурі за вимогами ISO 9001. Велика частина документації, необхідна за ISO 27001 вже могла бути розроблена і використовуватися в рамках ISO 9001.

Розробляється документація:

1. Сферах поширення СМІБ.
2. Політика в області ІБ.
3. Цілі.
4. Внутрішні цілі.
5. Керівництво з ІБ.
6. Заява про застосування контролю.
7. Розподіл відповідальності.
8. Таблиця оцінки ризиків.
9. План обробки ризиків.
10. Заява про прийняття остаточних ризиків.
11. Процедури «управління документацією», «управління записами».
12. Процедура «внутрішні перевірки».
13. Процедура «попереджувальні та коригуючі заходи».
14. Процедура ІБ.
15. Посадові інструкції.
16. Методичні та робочі інструкції.
17. Записи [1, 2].

2.4. Відповідальність керівництва

Найвищий рівень керівництва в будь-якій державній організації і компанії несе відповідальність за надійну, цілеспрямовану роботу відділів, і тому відповідає також за гарантію внутрішньої і зовнішньої безпеки ІТ. Залежно від типу організації і відділу вони можуть регулюватися різними законами. Отже, керівництво несе відповідальність за запуск, контроль і спостереження за процесом безпеки ІТ. Відповідальність за безпеку ІТ залишається на цьому рівні, але роль «відповідальний з ІТ безпеки» зазвичай призначається співробітнику Служби безпеки ІТ. При цьому керівництво повинно інтен-

екстреної необхідності. Це повинно поєднуватися з тестами процедур відновлення і перевіркою на відповідність необхідному часу відновлення. Тестування можливості відновити збережені дані на виділених для тестування носіях, а не перезаписом інформації на оригінальні носії в разі, якщо в процесі резервного копіювання або відновлення стався збій або виявилися невідновні пошкодження або втрата даних;

е) в тих випадках, коли важлива конфіденційність, дані, що резервуються повинні бути захищені криптографічними засобами.

Робочі процедури повинні передбачати контроль виконання резервного копіювання та обробку збоїв в ході виробленого за графіком резервного копіювання, щоб гарантувати завершення всіх операцій резервного копіювання відповідно до відповідної політики.

Заходи щодо створення резервної копії для конкретних систем або служб повинні регулярно тестуватися для гарантії того, що вони відповідають вимогам плану із забезпечення безперервності бізнесу. Для систем і служб, що мають критично важливе значення, заходи щодо створення резервної копії повинні охоплювати всю системну інформацію, додатки та дані, необхідні для відновлення всієї системи в разі аварійної ситуації.

Повинен бути визначений термін зберігання суттєвої для бізнесу інформації з урахуванням будь-яких вимог до архівування копій, які повинні постійно зберігатися.

Ведення журналів аудиту та моніторинг

Ціль: Записувати події та генерувати докази.

1) Журнал аудиту подій. Журнал аудиту подій, у якому записується діяльність користувачів, винятки, збої та події ІБ, треба вести, зберігати й регулярно переглядати.

Записи про події повинні включати, наскільки це може бути застосовано:

а) ідентифікатор користувача;

б) дії в системі;

в) дату, час і деталі ключових подій, наприклад, входу в систему і виходу з неї;

г) позначення пристрою або розміщення, якщо є така можливість, а також системний ідентифікатор;

д) записи успішних та відхилених системою спроб доступу;

Необхідно потурбуватися про те, щоб шкідливий код не був впроваджений в ході обслуговування і дій в аварійній ситуації, які можуть проводитися в обхід звичайних заходів щодо захисту від шкідливого коду.

Застосування в якості засобу захисту від шкідливого коду тільки програм, які виявляють і відновлюють зазвичай недостатньо і потрібні додаткові робочі процедури, які запобігають впровадження шкідливого коду.

Резервне копіювання

Ціль: Захистити від втрати даних.

Резервне копіювання інформації. Згідно із затвердженою політикою резервного копіювання треба регулярно робити і в подальшому тестувати резервні копії інформації, ПЗ та образів систем.

Повинна бути встановлена політика резервного копіювання, щоб визначити вимоги організації до резервного копіювання інформації, ПЗ і систем. Політика резервного копіювання повинна визначати вимоги щодо захисту і термінів зберігання.

Повинні бути надані відповідні пристрої для резервного копіювання з гарантією того, що істотна інформація та ПЗ можуть бути відновлені після аварійної ситуації або збою носія.

При формуванні плану резервного копіювання повинно бути враховано наступне:

а) повинні робитися точні і повні записи резервних копій і бути розроблені задокументовані методики відновлення;

б) обсяг (наприклад, повне або часткове копіювання) і частота резервного копіювання повинні відповідати бізнес-вимогам організації, вимогам з безпеки інформації, що зберігається, і важливості цієї інформації для забезпечення безперервності діяльності організації;

в) резервні копії повинні зберігатися у віддалених місцях, на суттєвій відстані для уникнення пошкодження в разі аварійних ситуацій в основному офісі;

г) резервованій інформації повинен бути забезпечений відповідний рівень захисту, як фізичних, так і від загроз зовнішнього впливу, відповідно до стандартів, що застосовуються в основному офісі;

д) носії для резервних копій повинні регулярно тестуватися для гарантії того, що на них можна покластися при застосуванні в разі

сивно залучатися до «процес управління безпекою ІТ». Тільки таким чином управління безпекою ІТ може гарантувати відсутність необгрунтованих ризиків і належне інвестування та забезпечення ресурсами. Найвищий рівень керівництва – інстанція, яка приймає рішення щодо управління ризиками й повинна забезпечувати відповідні ресурси.

Факт, що керівництво несе відповідальність за запобігання й управління ризиками ІТ-безпеки, часто не усвідомлюється вчасно. Це означає, що відповідальність за проблеми ІТ-безпеки часто не визначена. Після того, як трапиться інцидент у системі безпеки ІТ, оперативна інформація про потенційні ІТ-ризики може бути відзначена керівництвом або директором держустанови як відповідальність тих, хто відповідає за ІТ. З цієї причини рекомендується відповідальним за ІТ повідомляти керівництву про потенційні ризики і наслідки помилок безпеки ІТ. Однак, керівництво завжди відповідає за те, що воно отримує інформацію у відповідний час і у відповідному обсязі. Проблеми, пов'язані з безпекою, включають:

– ризики безпеки для організації та її інформації, включаючи опис пов'язаних результатів і витрат;

– результати події в системі безпеку ІТ в важливих бізнес-процесах повинні бути описані;

– вимога безпеки, обумовлені законом або договірними умовами, повинні бути описані;

– звичайні, стандартні підходи до безпеки ІТ в галузі повинні бути представлені;

– переваги сертифікації, включаючи показ досягнутого рівня ІБ, повинні бути пояснені клієнтам, бізнес-партнерам і контролюючим організаціям.

Оскільки третім сторонам, які не залучені, часто надають більше значення, ніж своєму персоналу, доцільно використовувати зовнішніх консультантів для підвищення розуміння ІТ-безпеки керівництва або директорів держустанов.

Хоча керівництво несе відповідальність за досягнення цілей системи безпеки, усі співробітники організації повинні бути залучені до процесу забезпечення безпеки. Ідеально було б дотримуватися таких принципів:

– ініціатива організації безпеки ІТ повинна виходити від адміністрації або керівництва;

– керівництво зберігає повну відповідальність за безпеку ІТ;

– функція «безпеку ІТ» має активно підтримуватися адміністрацією або керівництвом;

– адміністрація або керівництво призначають співробітників, відповідальних за безпеку ІТ і забезпечують їх необхідними навичками та ресурсами;

– керівництво подає приклад в тому, що стосується ІТ-безпеки. Це включає суворе дотримання керівництвом обумовлених правил безпеки.

Насамперед керівництво повинно гарантувати, що безпека ІТ інтегрована в усі важливі бізнес-процеси, процедури і проекти фахівців. Досвід показав, що співробітники Служби безпеки ІТ потребують повної підтримки керівництва.

Керівництво повинно визначити цілі управління безпекою ІТ та інших проблем так, щоб бажаний рівень безпеки ІТ був досяжний у всіх сферах за допомогою наданих ресурсів (персонал, час, гроші).

Менеджмент повинен забезпечувати докази своєї діяльності по створенню, забезпеченню, управлінню, моніторингу, контролю, підтримки та поліпшення СМІБ шляхом:

а) встановлення ролей і відповідальності за ІБ;

б) розробки політики СМІБ;

в) створення оргструктури (див. рис. 2.8-2.10);

г) аналізу СМІБ;

д) забезпечення ресурсами.

Менеджмент повинен затвердити (розробити) політику і цілі у сфері ІБ.

а) Наявність факту затвердження документів.

б) Наявність дати затвердження.

Установка ролей і відповідальності.

Відповідальність за функціонування системи менеджменту ІБ.

ж) установка і регулярне оновлення програм виявлення шкідливого коду і відновлення для сканування комп'ютерів і носіїв в якості запобіжного заходу або на постійній основі; сканування повинне виконуватися, включаючи:

1) сканування на предмет шкідливого коду будь-яких файлів, отриманих по мережі або через будь-які носії інформації, до їх використання;

2) сканування на предмет шкідливого коду вкладень до повідомлень електронної пошти і завантажених файлів до їх використання. Таке сканування має проводитися в різних місцях, наприклад, на поштових серверах, настільних комп'ютерах і на апаратурі підключення організації до мережі;

3) сканування на предмет шкідливого коду веб-сторінок;

з) визначення обов'язків і процедур для забезпечення захисту від атак шкідливого коду, навчання їх застосуванню, складання звітів і відновленню після атак шкідливого коду;

и) підготовка відповідних планів безперервності бізнесу для відновлення після атак шкідливого коду, включаючи всі необхідні дані і програми резервного копіювання, а також заходи щодо відновлення;

к) виконання процедур регулярного збору інформації, таких як підписка на розсилки або відвідування ресурсів з інформацією про нові шкідливі програми;

л) виконання процедур перевірки інформації, пов'язаної з шкідливими програмами, і гарантування того, що попереджувальні повідомлення точні і інформативні. Керівники повинні гарантувати, що для відділення реальних шкідливих програм від помилкових використовуються кваліфіковані джерела, наприклад, авторитетні журнали, надійні Інтернет-сайти або постачальники, що виробляють ПЗ для захисту від шкідливих програм. Всі користувачі повинні бути сповіщені про проблему помилкових шкідливих програм і що необхідно робити при їх отриманні;

м) ізолювання середовищ, в яких наслідки можуть бути катастрофічними.

Застосування двох або більше програмних продуктів, що захищають від шкідливих програм в системах обробки інформації, від різних виробників і реалізують різні технології може підвищити результативність захисту від шкідливого коду.

Персонал, що виконує розробку і тестування, також становить загрозу для конфіденційності робочої інформації. Дії в ході розробки та тестування можуть викликати ненавмисні зміни в ПЗ або інформації, якщо вони виконуються в одному обчислювальному середовищі. Таким чином, бажано поділ середовища розробки, тестування та робочого середовища для зниження ризику випадкової зміни або неавторизованого доступу до робочого ПЗ або робочих даних.

Захист від зловмисного коду

Ціль: Гарантувати, що інформація та засоби оброблення інформації захищені від зловмисного коду.

Заходи безпеки проти зловмисного коду. Має бути впроваджено заходи безпеки щодо виявлення, запобігання та відновлення для захисту від зловмисного коду і належні процедури поінформування користувачів.

Захист від шкідливого коду повинен ґрунтуватися на застосуванні програм виявлення шкідливого коду і відновлення, обізнаності про ІБ та відповідних засобах контролю доступу до системи та управління змінами. Повинні бути прийняті до уваги наступні рекомендації:

а) розробка офіційної політики, яка забороняє використання неавторизованого ПЗ;

б) впровадження заходів, які запобігають або виявляють застосування неавторизованого ПЗ (наприклад, ведення списку дозволених програм);

в) впровадження заходів, які запобігають або виявляють звернення до відомих шкідливих або підозрілих веб-сайтів (наприклад, ведення чорних списків таких сайтів);

г) розробка офіційної політики для захисту від ризиків, пов'язаних з отриманням файлів і ПЗ, через зовнішні мережі чи будь-які інші середовища, із зазначенням, які захисні заходи мають бути вжиті;

д) зменшення уразливостей, які могли б бути використані шкідливим кодом, наприклад, за допомогою управління технічними уразливостями;

е) проведення регулярних перевірок ПЗ і даних систем, що підтримують важливі бізнес-процеси. Присутність будь-яких несанкціонованих файлів і змін має офіційно розслідуватися;

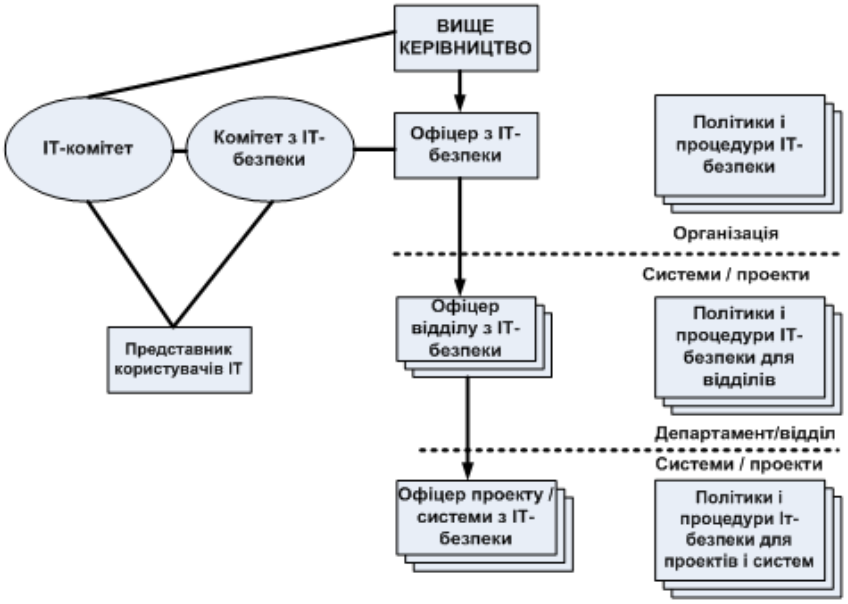


Рис. 2.8. Приклад структури організації IT-безпеки у великих установах

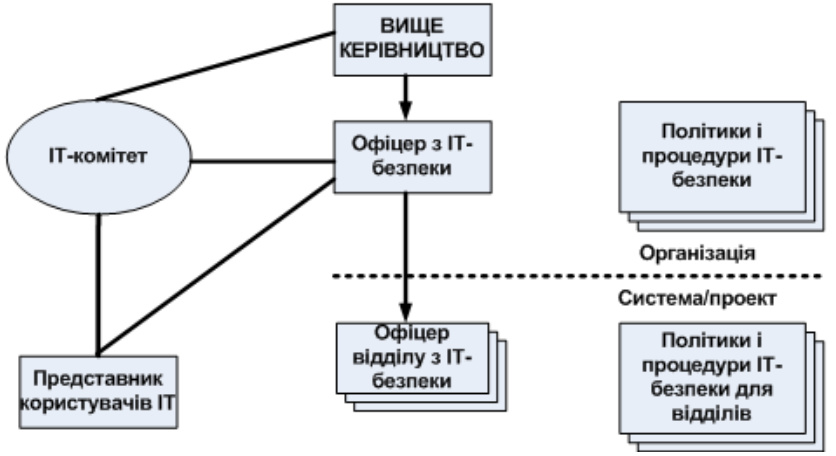


Рис. 2.9. Приклад структури організації IT-безпеки у середніх установах

Рис. 2.10. Приклад структури організації ІТ-безпеки у малих установах

Менеджмент повинен забезпечувати свідчення своєї діяльності зі створення, забезпечення, управління, моніторингу, контролю, підтримки та поліпшення СМІБ шляхом:

...

Встановлення ролей і відповідальність за ІБ

...

Приклад встановлення ролей: відповідальність за функціонування системи менеджменту ІБ:

- Керівник служби безпеки.
- Керівник служби якості.
- Керівник служби ІТ.
- Керівник служби ІТ безпеки.
- Перший керівник.

Організація повинна визначати зовнішні та внутрішні проблеми, що мають відношення до її мети та впливають на здатність досягти передбачуваного результату в СМІБ.

Вище керівництво повинно демонструвати лідерство та виконувати зобов'язання щодо СМІБ шляхом:

а) забезпечення політики та цілей ІБ, що є встановленими та сумісними з стратегічним напрямом діяльності організації;

б) забезпечення інтеграції вимог СМІБ в процеси організації;

в) забезпечення наявності ресурсів, необхідних для СМІБ;

г) донесення важливості ефективного управління ІБ та відповідності вимогам СМІБ;

д) гарантування досягнення СМІБ передбачуваних результатів;

е) координування та підтримкою осіб, що сприяють ефективності СМІБ;

Повинен бути визначений і реалізований необхідний для запобігання виникненню проблем функціонування рівень поділу середовища розробки, тестування та робочого середовища.

Повинно бути прийнято до уваги наступне:

а) повинні бути визначені і документовані правила переходу ПЗ зі статусу розробки в статус придатності до експлуатації;

б) середовище розробки і робоче середовище повинні бути запущені в різних системах або на різних комп'ютерах і в різних доменах або директоріях;

в) зміни в робочих системах і застосунках повинні тестуватися у тестовому або проміжному середовищі до того, як вони будуть застосовані до робочих систем;

г) не повинно проводитися тестування на робочих системах, крім як у випадку виникнення виключень;

д) компілятори, редактори та інший інструментарій для розробки або системні утиліти не повинні бути доступні з робочих систем, коли в цьому немає необхідності;

е) користувачі повинні використовувати різні профілі користувачів для робітників і тестових систем і на екрані повинні відображатися відповідні попереджувальні повідомлення для зниження ризику помилки;

ж) конфіденційні дані не повинні копіюватися в середу тестування систем, якщо тільки не забезпечені для тестованої системи належні засоби контролю.

Дії в ході розробки та тестування можуть викликати серйозні проблеми, наприклад, небажане зміна файлів або системного середовища, або системні збої. Є необхідність підтримувати зрозуміле і стабільне середовище для виконання повноцінного тестування і запобігання несанкціонованого доступу розробників до робочого середовища.

Там, де персонал, який виконує розробку і тестування, має доступ до робочого середовища і її інформацією, він може мати можливість впровадити неавторизований та не тестований код або альтернативні робочі дані. На деяких системах така можливість могла б бути використана для здійснення обману або застосування не протестованого або шкідливого коду, що може викликати серйозні проблеми в експлуатації.

Вимоги до продуктивності повинні бути визначені з урахуванням важливості розглянутої системи для бізнесу. Повинні проводитися настройка і моніторинг системи, щоб гарантувати і, де необхідно, покращувати придатність і ефективність систем. Повинні бути задіяні засоби виявлення для своєчасного виявлення проблем. Прогнози вимог до продуктивності в майбутньому повинні враховувати нові вимоги як з боку бізнесу, так і систем, а також поточні та прогнозовані тенденції в можливостях обробки інформації в організації.

Особливу увагу потрібно приділити ресурсам з тривалим терміном отримання або з високою вартістю, тому керівники повинні здійснювати контроль за використанням ключових ресурсів системи. Вони повинні виявляти тенденції у використанні, особливо, пов'язані з бізнес-додатками або інструментарієм управління ІС. Керівники повинні використовувати цю інформацію для виявлення і усунення потенційних вузьких місць і залежностей від ключового персоналу, які можуть становити загрозу безпеці систем або служб, а також планувати відповідні дії.

Забезпечення достатньої продуктивності може бути досягнуто як збільшенням можливостей, так і зниженням запитів. Приклади управління запитами включають в себе:

а) видалення застарілих даних (обсяг диска);

б) деінсталяцію застосунків, систем, баз даних або середовищ;

в) оптимізацію пакетних завдань і їх розкладу;

г) оптимізацію алгоритмів додатків або запитів до баз даних;

д) відмова в наданні або обмеження смуги пропускання для ресурсномістких служб, якщо вони не важливі для бізнесу (наприклад, потокове відео).

Повинна бути розглянута можливість документованого плану управління продуктивністю для критично важливих систем.

Розглянуті заходи також застосовні до людських ресурсів, так само як і до офісів і обладнання.

4) Відокремлення засобів розробки, тестування та експлуатації. Засоби розроблення, тестування та експлуатації має бути відокремлено для зменшення ризиків несанкціонованого доступу чи змін в операційному середовищі.

ж) сприяння безперервному вдосконаленню;

з) підтримка інших відповідних управлінських ролей, що продемонстрували своє лідерство, у сферах їх відповідальності.

Вище керівництво повинне забезпечити призначення обов'язків щодо функцій, що стосуються ІБ, та проінформувати про них та відповідальність співробітників.

Вище керівництво призначає відповідальність та повноваження для:

а) забезпечення відповідності СМІБ вимогам Міжнародного Стандарту;

б) звітності керівництву про ефективність СМІБ.

Вище керівництво також може покласти відповідальність і наділити повноваженнями для інформування про функціонування СМІБ у межах організації [1, 2].

2.5. Цілі інформаційної безпеки та планування їх досягнення

Процес планування кінцевого впровадження СМІБ включає п'ять фаз (див. рис. 2.11). Ці п'ять фаз такі:

а) отримання схвалення керівництва для запуску проекту СМІБ;

б) визначення сфери дії і політики СМІБ;

в) проведення аналізу організації;

г) проведення аналізу ризиків та планування обробки ризиків;

д) розробка СМІБ [3].

На рис. 2.11 представлені п'ять фаз планування проекту СМІБ із зазначенням основних вихідних документів.

Дії

Цілі впровадження СМІБ повинні враховуватися при розгляді пріоритетів і вимог організації до ІБ.

Вихідні дані:

а) стратегічні цілі організації;

б) огляд існуючих систем управління;

в) перелік правових, нормативних та договірних вимог до ІБ, які застосовуються в організації.

Рекомендації

Для запуску проекту СМІБ зазвичай потрібне схвалення керівництва. Отже, перша дія, яку необхідно виконати – збір суттєвої інформації, яка б показала значення СМІБ для організації. Органі-

зація повинна визначити, навіщо потрібна СМІБ, визначити цілі впровадження СМІБ і запустити проект СМІБ.

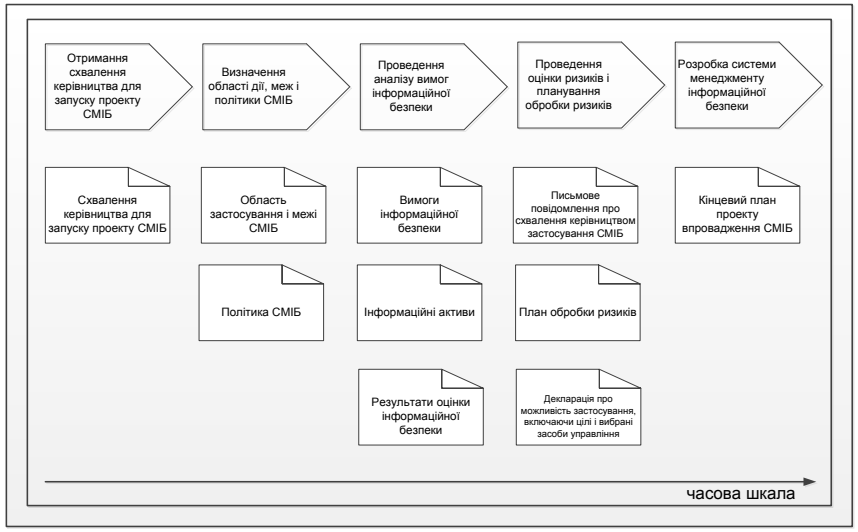


Рис. 2.11. Фази проекту СМІБ

Цілі впровадження СМІБ можна визначити, відповівши на наступні питання:

а) менеджмент ризику – як може СМІБ поліпшити управління ризиками для ІБ?

б) результативність – як може СМІБ поліпшити управління ІБ?

в) переваги для підприємства – як може СМІБ створити конкурентні переваги для організації?

Щоб відповісти на ці запитання, необхідно розглянути пріоритети і вимоги організації у сфері ІБ на основі наступних чинників:

а) найважливіші сфери діяльності підприємства і організації:

1) Що є найважливішими сферами діяльності підприємства і організації?

2) Які сфери діяльності організації забезпечують ведення бізнесу і чому приділяється особлива увага?

3) Які існують взаємини і угоди з третіми сторонами?

4) Чи залучаються сторонні організації для надання будь-яких послуг?

б) засекречена або цінна інформація:

и) управління інформацією, що міститься в журналах перевірок і системних журналах;

к) процедури моніторингу.

Робочі процедури та задокументовані методики з системними операціями повинні розглядатися як офіційні документи і зміни в них затверджуватися керівництвом. Там, де це технічно можливо, ІС повинні управлятися єдиним чином, із застосуванням одних процедур, інструментів та утиліт.

2) Управління змінами. Зміни в організації, бізнес-процесах, засобах оброблення інформації та системах, які впливають на ІБ, мають бути контрольованими.

Зокрема, має бути прийнято до уваги наступне:

а) ідентифікація і реєстрація істотних змін;

б) планування і тестування змін;

в) оцінка потенційного впливу здійснюваних змін, включаючи вплив на ІБ;

г) процедура офіційного затвердження запропонованих змін;

д) підтвердження, що вимоги з ІБ виконані;

е) інформування про зміни всіх зацікавлених осіб;

ж) процедури відкоту до початкового стану, включаючи процедури і обов'язки з зупинки і відновленню після невдалих змін і непередбачених подій;

з) наявність процесу термінових змін для забезпечення швидкого і контрольованого виконання змін, необхідних для усунення інциденту.

Повинні бути розроблені формалізовані процедури управління і встановлена відповідальність для гарантії належного контролю змін. При виконанні змін в контрольному журналі повинна зберігатися вся необхідна інформація.

Невідповідний контроль змін в засобах обробки інформації та системах є типовою причиною системних збоїв або порушень безпеки. Зміни в операційному середовищі, особливо при переході системи зі стадії розробки на стадію експлуатації, можуть впливати на надійність застосунків.

3) Управління потужністю. Для забезпечення потрібної продуктивності системи необхідно здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності.

Слід розглянути можливість використання друкуючих пристроїв з функцією PIN-коду, коли тільки автор документа може його отримати, перебуваючи безпосередньо у принтера [1, 2].

4.8. Безпека виробничих процесів

Процедури експлуатації та відповідальності

Ціль: Забезпечити коректне та безпечне функціонування засобів оброблення інформації.

1) Документовані процедури експлуатації. Процедури експлуатації має бути задокументовано та зроблено доступними для всіх користувачів, що їх потребують.

Повинні бути розроблені робочі процедури для повсякденної діяльності, пов'язаної з обладнанням обробки інформації та засобами зв'язку, такі, як процедури включення і виключення комп'ютерів, резервного копіювання, обслуговування устаткування, роботи з носіями, управління і забезпечення безпеки в комп'ютерному залі і при обробці пошти.

Ці робочі процедури повинні містити інструкції щодо виконання дій, включаючи:

а) встановлення та конфігурацію систем;

б) ручну і автоматичну обробку інформації;

в) резервне копіювання;

г) вимоги до планування, в тому числі і з урахуванням зв’язків з іншими системами, терміну початку першої роботи і терміну закінчення останньої;

д) інструкції з обробки помилок або інших виняткових ситуацій, які можуть виникнути в ході роботи, включаючи обмеження на використання системних утиліт;

е) технічну підтримку і контакти для передачі проблеми на вищий рівень, включаючи контакти зовнішніх служб забезпечення, в разі відхилень від очікуваного функціонування або виникнення технічних складнощів;

ж) інструкції щодо поводження з особливими носіями і особливими даними, наприклад, з використання спеціальних бланків або управління виводом конфіденційної інформації, включаючи знищення результатів виведення в разі невдалого виконання операції;

з) перезапуск системи і процедури відновлення у разі збою в системі;

1) Яка інформація є найбільш важливою для організації?

2) Якими могли б бути можливі наслідки у разі розголошення певної інформації не уповноваженим сторонам (наприклад, втрата конкурентних переваг, збиток щодо бренда або репутації, судовий позов і т.ін.)?

в) закони, які роблять привабливим впровадження заходів ІБ:

1) Які закони застосовуються в організації, що регламентують обробку ризику чи ІБ?

2) Чи є організація публічної глобальною організацією, для якої потрібна зовнішня фінансова звітність?

г) контрактні або організаційні угоди, які стосуються ІБ:

1) Які вимоги пред'являються до зберігання даних (включаючи терміни зберігання)?

2) Чи існують контрактні вимоги, пов'язані з секретністю або якістю (наприклад, угода за рівнем послуг – SLA)?

д) галузеві вимоги, що визначають конкретні способи управління і заходи ІБ:

1) Які вимоги, характерні для даної галузі, застосовуються до організації?

е) загрози:

1) Які потрібні види захисту і від яких загроз?

2) Для яких окремих категорій інформації потрібен захист?

3) Які окремі види інформаційної діяльності вимагають захисту?

ж) Конкурентні рушійні фактори:

1) Які мінімальні вимоги до ІБ існують на ринку?

2) Які додаткові способи менеджменту ІБ можуть бути стимульовані конкурентними перевагами організації?

з) вимоги безперервності бізнес-процесів:

1) Які існують найважливіші бізнес-процеси?

2) Як довго організація може витримувати припинення кожного з найважливіших бізнес-процесів?

Попередню сферу дії СМІБ можна визначити, відповівши на наведені вище питання. Детальна сфера дії СМІБ повинна бути визначена під час складання проекту СМІБ.

Приклади цілей управління, які можуть використовуватися як вихідні дані для визначення попередньої сфери дії СМІБ, включають:

а) сприяння безперервності бізнес-процесів і відновленню їх в надзвичайних ситуаціях;

б) підвищення стійкості до інцидентів;

в) увагу до відповідності законам (умовам) контракту та зобов'язаннями;

г) забезпечення можливості сертифікації за іншими стандартами ISO/IEC;

д) забезпечення розвитку і положення організації;

е) зниження витрат на управління безпекою;

ж) захист стратегічно важливих активів;

з) створення сприятливого та ефективного середовища внутрішнього управління;

и) забезпечення впевненості зацікавлених сторін в тому, що інформаційні активи відповідним чином захищені.

Вихідні дані

Вихідні дані після виконання цієї дії наступні:

а) документ, що відображає цілі, пріоритети у сфері ІБ і вимоги організації до СМІБ;

б) перелік законних, контрактних і галузевих вимог до ІБ організації;

в) опис характеристик підприємства, організації, місцезнаходження, активів і технологій [3].

Визначення вимог захисту (визначення цілей)

Визначення вимог захисту зареєстрованої ІТ-структури може складатися, наприклад, з чотирьох окремих кроків. На перших кроках реалізовується визначення категорій вимог безпеки використовуючи стандартні сценарії порушень для бізнес-процесів та ІТ-додатків, які їх підтримують. Потім з результатів отримують вимоги безпеки окремих ІТ-систем. У свою чергу, ці результати визначають вимоги безпеки для шляхів передачі і ділянок, які використовуються для ІТ.

Визначення вимог безпеки для ІТ-додатків

Метою визначення вимог безпеки, починаючи з бізнес-процесів, є вирішення для кожного зареєстрованого ІТ-додатку, включаючи їх дані, які вимоги безпеки для конфіденційності, цілісності та доступності. Ці вимоги безпеки орієнтовані на потенційні порушення, пов'язані з несприятливим впливом на ІТ-додаток і, відповідно, на відповідні бізнес-процеси.

а) розривати активну сесію після завершення роботи, якщо тільки вона не може бути захищена відповідним блокуючим механізмом;

б) виходити з додатків або мережевих служб, коли в них більше немає необхідності;

в) захищати комп'ютери або мобільні пристрої від несанкціонованого використання замиканням на ключ або схожим способом, наприклад, доступом за допомогою паролю, коли пристрій не використовується.

9) Політика чистого стола та чистого екрана. Повинні бути ухвалені політика чистого стола щодо паперів і змінних носіїв інформації та політика чистого екрана щодо засобів оброблення інформації.

Політика чистого стола та чистого екрана повинна враховувати категорії інформації, законодавчі та контрактні вимоги, а також відповідні ризики і корпоративну культуру організації. Слід враховувати наступні рекомендації:

а) уразлива або критично важлива для бізнесу інформація, наприклад, на папері або на електронних носіях, повинна зберігатися замкненою (ідеально – в сейфі чи шафі, або іншому предметі меблів, що забезпечує захист), поки не використовується, особливо, якщо в офісі нікого немає;

б) комп'ютери і термінали, залишені без нагляду, повинні залишатися в стані виконаного виходу з системи або захищеними механізмом блокування екрану і клавіатури, керованим паролем, апаратним ключем або подібним засобом автентифікації користувача, і повинні бути блоковані ключем, паролями або іншими засобами, коли не використовуються;

в) не повинно допускатися несанкціоноване використання копіювальних апаратів та інших відтворюючих пристроїв (наприклад, сканерів, цифрових камер);

г) відбитки, які містять уразливу або класифіковану інформацію, необхідно забирати з друкуючих пристроїв негайно.

Політика чистого стола / чистого екрана знижує ризик несанкціонованого доступу, втрати або пошкодження інформації в робочий і позаробочий час. Сейфи та інші пристрої надійного зберігання могли б також захистити збережену в них інформацію від таких загроз, як пожежа, землетрус, повінь або вибух.

або ліцензійне ПЗ було видалено чи безпечним чином перезаписано до вилучення або повторного використання.

Обладнання повинно бути перевірено до утилізації або повторного використання з метою з'ясувати, чи містяться в ньому накопичувачі чи ні.

Накопичувачі, що містять конфіденційну або захищену авторськими правами інформацію, повинні бути фізично зруйновані або інформація повинна бути стерта, видалена або переписана із застосуванням технологій, які роблять неможливим відновлення оригінальної інформації, а не використанням стандартних функцій видалення або форматування.

Для пошкодженого обладнання, що містить носії, може знадобитися оцінка ризиків, щоб визначити, чи повинен бути цей елемент швидше знищений, ніж відданий в ремонт або викинутий. Інформація може бути скомпрометована через неналежну утилізації або повторного застосування обладнання.

Крім того, для надійного очищення диска шифрування всієї інформації на диску знижує ризик розкриття конфіденційної інформації в тих випадках, коли обладнання йде на утилізацію або повторне використання за умови, що:

а) шифрування досить сильне і охоплює весь диск (включаючи незайняті частини кластерів, своп-файли і т.д.);

б) ключі шифрування досить довгі, щоб протистояти атакам методом підбору;

в) самі ключі шифрування зберігаються надійно (наприклад, ніколи не зберігаються на тому ж диску).

Методи надійного перезапису накопичувачів відрізняються в залежності від технології, що застосовується в носіях інформації. Необхідно проаналізувати інструменти перезапису, щоб переконатися, що вони можуть бути застосовані до конкретної технології.

8) Обладнання користувачів, залишене без нагляду. Користувачі мають забезпечити, що залишене без нагляду обладнання, належним чином захищене.

Всі користувачі повинні бути обізнані з вимогами безпеки і процедурами для захисту обладнання, яке залишається без нагляду, так само як і про їхню відповідальність за забезпечення такого захисту. Користувачам має бути рекомендовано:

Оскільки вимоги безпеки здебільшого незліченні, то IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodology) [4] поділяє вимоги безпеки на три категорії (див. табл. 2.1).

Таблиця 2.1. Категорії вимог безпеки

Вимоги безпеки	Характеристика
«нормальні»	Вплив будь-якої втрати або порушення обмежений і може бути вимірюваний
«високі»	Вплив будь-якої втрати або порушення може бути значним
«дуже високі»	Вплив будь-якої втрати або порушення може досягати катастрофічних розмірів, які можуть загрожувати існуванню

Наступні кроки описують, як визначити відповідну категорію вимог безпеки для бізнес-процесу і відповідних IT-додатків.

Крок 1: Визначення категорій вимог безпеки

Пошкодження, які можуть статися, якщо конфіденційність, цілісність або доступність будуть втрачені для певного бізнес-процесу або для IT-додатка, включаючи його дані, які зазвичай можуть відповідати таким сценаріям:

- Порушення законів, нормативів, контрактів.
- Зниження інформаційного самовизначення.
- Фізичні пошкодження.
- Порушення виконання обов'язків.
- Негативне внутрішнє або зовнішнє вплив.
- Фінансові наслідки.

Часто, єдиний випадок втрати або порушення може залучити кілька категорій пошкоджень. Тому, наприклад, збій може перешкоджати виконанню важливого IT-додатку, що призведе до фінансових втрат і, як наслідок, до втрати репутації.

Щоб розрізняти «нормальну», «високу» і «дуже високу» категорії вимог безпеки, може бути доречним визначити межі для окремих сценаріїв пошкодження. Наступні таблиці 2.2-2.4 використовуються для визначення потенційних ушкоджень та їх наслідків для кожної вимоги безпеки. Кожна організація повинна відкоригувати ці таблиці під власні умови.

Таблиця 2.2. Вимоги безпеки категорії «нормальні»

Сценарії пошкодження	Наслідки
1. Порушення законів, нормативів або контрактів	- порушення нормативів і законів з мінімальними наслідками; - мінімальні порушення контракту, які спричиняють незначні договірні неустойки.
2. Зниження прав на інформаційне самовизначення	- зниження прав на інформаційне самовизначення розцінюється людиною як терпиме; - можливе зловживання людиною, що має відношення до даних, має мінімальний вплив на соціальне або фінансове становище зацікавлених осіб.
3. Фізичні ушкодження	- не здається можливим.
4. Порушення виконання обов'язків	- порушення розцінюється як терпиме зацікавленими особами; - максимально допустимий час простою більше 24 годин.
5. Негативний внутрішній або зовнішній вплив	- мінімальне зниження репутації / довіри, в межах установи / підприємства.
6. Фінансові наслідки	- фінансові втрати прийнятні для організації.

Таблиця 2.3. Вимоги безпеки категорії «високі»

Сценарії пошкодження	Наслідки
1. Порушення законів, нормативів або контрактів	- порушення нормативів і законів зі значними наслідками; - більшість порушень контракту тягнуть значні договірні неустойки.
2. Зниження прав на інформаційне самовизначення	- можливе значне зниження індивідуальних прав на інформаційне самовизначення; - можливе зловживання даними, пов'язаними з людьми, буде мати значний вплив на соціальне або фінансове становище зацікавлених осіб.
3. Фізичні ушкодження	- можливі фізичні ушкодження окремих осіб.
4. Порушення виконання обов'язків	- порушення виконання обов'язків розцінюється, як нетерпиме деякими зацікавленими особами; - максимально допустимий час простою від 1 до 24 годин.
5. Негативний внутрішній або зовнішній вплив	- можливе значне зниження репутації / довіри.
6. Фінансові наслідки	- фінансові втрати значні, але організація може «вижити».

Використання за межами організації будь-якого обладнання, яке обробляє або зберігає інформацію, має бути дозволено керівництвом. Це відноситься до обладнання яке належить організації, так і до особистого, але використовуваному в інтересах організації.

Для захисту обладнання поза організацією повинні бути прийняті до уваги наступні рекомендації:

а) обладнання і носії, що виносяться за межі організації, не повинні залишатися без нагляду в громадських місцях;

б) інструкції виробника щодо захисту обладнання повинні завжди дотримуватися, наприклад, захист від впливу сильних електромагнітних полів;

в) заходи для роботи поза офісом, таких як робота вдома, віддалена робота або робота на тимчасовому місці, повинні бути визначені на основі оцінки ризиків та застосовані відповідні ситуації методи, наприклад, шафи, що закриваються для зберігання документів, політика чистого столу, контроль доступу до комп'ютерів і захист ліній зв'язку з офісом);

г) в тих випадках, коли обладнання, що знаходиться поза територією організації, передається один одному різними людьми або зовнішніми сторонами, повинен вестися журнал, який реєструє всю послідовність передачі обладнання, включаючи, як мінімум, прізвища та назви організацій тих, хто несе відповідальність за обладнання.

Ризики, пов'язані, наприклад, з пошкодженням, крадіжкою або прослуховуванням, можуть істотно відрізнятися в залежності від місця та повинні враховуватися при визначенні найбільш доцільних заходів.

Обладнання, яке обробляє або зберігає інформацію, включає в себе всі види персональних комп'ютерів, органайзерів, мобільних телефонів, смарт-карт, паперові документи та інші види носіїв, які зберігаються для роботи вдома або виносяться з звичайного місця роботи.

Можливо, буде доцільно зменшити ризик, переконавши певних співробітників не працювати поза офісом або обмеживши використання ними портативного IT-обладнання.

7) Безпечне вилучення або повторне використання обладнання. Всі елементи обладнання, які містять носії пам'яті, має бути перевірено для забезпечення того, що будь-які конфіденційні дані

г) в тих випадках, коли планується проведення обслуговування, повинні бути вжиті відповідні заходи з урахуванням того, чи будуть проводитися роботи на місці або в зовнішній організації, якщо необхідно, конфіденційна інформація повинна бути видалена з обладнання або обслуговуючий персонал повинен мати відповідний допуск;

д) всі вимоги до обслуговування, що накладаються договорами страхування, повинні бути виконані;

е) перед поверненням обладнання в експлуатацію повинна бути проведена перевірка, щоб гарантувати, що в обладнання не внесені незаконні зміни і воно функціонує нормально.

5) Переміщення активів. Обладнання, інформацію чи ПЗ не потрібно виносити назовні без попередньої санкції на ці дії.

Повинні бути прийняті до уваги наступні рекомендації:

а) повинні бути визначені співробітники і зовнішні користувачі, хто має право видавати дозволи на винос активів;

б) повинні бути встановлені терміни повернення активу і потім перевірено їх дотримання;

в) у тих випадках, коли необхідно і можливо, винос і повернення активу, повинні бути зареєстровані;

г) особистість, посаду і приналежність особи, яка керує активами або використовує їх, повинні бути задокументовані і ці документи повинні бути повернуті разом з обладнанням, інформацією або ПЗ.

Вибіркові перевірки, що проводяться для виявлення випадків несанкціонованого виносу активів, можуть також проводитися для виявлення недозволених записуючих пристроїв, зброї, а також для попередження їх пронесення на територію і виносу з території. Такі вибіркові перевірки повинні проводитися відповідно до чинного законодавства і регламентам. Персонал повинен бути поінформований про те, що проводяться вибіркові перевірки, і ці перевірки повинні проводитися в суворій відповідності з законодавчими та нормативними вимогами.

6) Безпека обладнання та активів СМІБ поза службовими приміщеннями. До активів СМІБ поза службовими приміщеннями має бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.

Таблиця 2.4. Вимоги безпеки категорії «дуже високі»

Сценарії пошкодження	Наслідки
1. Порушення законів, нормативів або контрактів	- дуже значні порушення нормативів і законів; - порушення контрактів з тяжкими наслідками.
2. Зниження прав на інформаційне самовизначення	- можливе особливе істотне порушення прав людини на інформаційне самовизначення; - можливі зловживання персональними даними, які можуть призвести до соціального або фінансового краху зацікавлених осіб.
3. Фізичні ушкодження	- можливі серйозні ушкодження окремих осіб; - небезпека для життя і частин тіла.
4. Порушення виконання обов'язків	- порушення виконання обов'язків розцінюється як неприпустиме усіма зацікавленими особами; - максимально допустимий час простою менше години.
5. Негативний внутрішній або зовнішній вплив	- можлива втрата репутації / довіри в масштабах нації або держави, можлива навіть загроза існуванню установи / компанії.
6. Фінансові наслідки	- установа / фірма не зможе вижити внаслідок фінансових втрат.

Кастомізація таблиці значень

В окремих випадках можливі інші сценарії ушкоджень, які не включені в шість сценаріїв, перерахованих вище, і в кожному випадку таблицю слід розширити відповідним чином. Для всіх пошкоджень, які не можуть бути описані в цих сценаріях, також необхідно встановити межі між «нормальні», «високі» та «дуже високі».

Крім того, повинні братися до уваги індивідуальні обставини організації. Втрата 200 000 € може бути досить незначною в порівнянні з оборотами і бюджетами IT у великій компанії, тоді як для маленької організації втрата навіть 10 000 € може привести до нездатності «вижити». Тому доречно визначити межі в процентах від загального обороту, загального доходу або IT бюджету.

Подібні міркування використовують щодо вимог доступності. Тому, наприклад, в деяких організаціях простій 24 години може бути допустимий. Але якщо буде декілька таких збоїв, наприклад, більш ніж раз на тиждень, результат може бути неприпустимим.

Під час обговорення меж між «нормальним», «високими» та «дуже високими», слід розглянути той факт, що стандарт IT-Grundschutz [4] для заходів захисту повинен відповідати звичайним вимогам безпеки. Обговорення необхідно документувати в концепції безпеки, тому що від цього залежить вибір заходів безпеки IT.

Крок 2: Розгляд сценаріїв пошкоджень

Починаючи від можливості втрати конфіденційності, цілісності або доступності IT-додатків або відповідної інформації, розглядають максимальне подальше пошкодження, яке може виникнути в такій ситуації. Використовуючи питання «Що трапиться, якщо ...?». Створюються реальні сценарії пошкодження *з точки зору користувача* й описуються очікувані матеріальні або нематеріальні збитки. Ступінь можливого пошкодження, у кінцевому рахунку, визначає вимоги безпеки IT-додатків. Важливо запитати особисту оцінку у відповідальних осіб і користувачів розглянутих IT-додатків. У них швидше за все будуть ідеї про те, які ушкодження відбулися, та вони зможуть зробити корисний внесок при зборі даних.

Щоб полегшити процес розрахунку можливого пошкодження, нижче надається набір питань для кожного згаданого сценарію пошкоджень, як інструмент для перевірки можливих впливів. Тут не стверджується, що ці пропозиції повні. Вони надаються як керівництво. В кожному випадку необхідно розглядати специфічну діяльність організації, а питання, наведенні вище, повинні відповідно доповнюватися.

Робота за допомогою сценаріїв пошкодження, перерахованих нижче, включаючи пов'язані з ним питання, рекомендується для кожного зареєстрованого IT-додатку. А таблиці 2.2-2.4 використовуються для визначення вимог безпеки щодо конфіденційності, цілісності й доступності, а потім призначається категорія вимог захисту.

Сценарій пошкодження «Порушення законів, нормативів або контрактів»

Такі пошкодження можуть стати результатом втрати конфіденційності, цілісності або доступності. Серйозність ушкодження залежить від певних юридичних наслідків для організації.

Приклади відповідного законодавства:

Повинні бути забезпечені аварійне живлення і зв'язок. Аварійні вимикачі і вентилі для відключення електрики, води, газу та інших видів постачання повинні розташовуватися поблизу аварійних виходів або приміщень з обладнанням.

Дублювання мережевих з'єднань може бути забезпечено декількома каналами зв'язку від більш, ніж одного провайдера послуг.

3) Безпека кабельних мереж. Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг має бути захищено від перехоплювання, взаємного впливу чи пошкоджень.

Для захисту кабельних мереж повинні бути прийняті до уваги наступні рекомендації:

а) телекомунікаційні лінії та лінії живлення пристроїв обробки інформації повинні бути підземними, де це можливо, або ж мати відповідний додатковий захист;

б) кабелі живлення і телекомунікаційні кабелі повинні бути прокладені окремо для виключення перешкод;

в) для уразливих і критично важливих систем повинні бути передбачені додаткові заходи, включаючи:

1) прокладку армованого кабелю, розташування точок входу кабелю в замкнених приміщеннях або ящиках;

2) застосування електромагнітних екранів для захисту кабелів;

3) проведення перевірок технічними засобами на місцях для виявлення пристроїв, підключених до кабелів;

4) контрольований доступ до сполучних панелей та комутаційних кімнатах.

4) Обслуговування обладнання. Обладнання потрібно правильно обслуговувати, щоб забезпечити його постійну доступність і цілісність.

При обслуговуванні обладнання повинні бути прийняті до уваги наступні рекомендації:

а) обладнання повинно обслуговуватися відповідно до заданих виробником періодів обслуговування і вимог;

б) ремонт та обслуговування обладнання повинен виконувати тільки авторизований обслуговуючий персонал;

в) повинні зберігатися записи про всі передбачувані або фактичні збої, а також про всі профілактичні і ремонтні роботи;

в) пристрої зберігання інформації повинні бути захищені від несанкціонованого доступу;

г) об'єкти, що вимагають спеціальних заходів захисту, повинні охоронятися, щоб знизити загальний рівень необхідного захисту;

д) повинні бути вжиті заходи для зниження ризику потенційних загроз фізичного і природного характеру, наприклад, крадіжки, пожежі, вибухи, задимлення, повені (або затоплення водою через аварію), запилення, вібрації, хімічний вплив, переривання електропостачання та зв'язку, електромагнітна радіація і вандалізм;

е) повинні бути встановлені правила прийому їжі та куріння в зонах, розташованих поруч з обладнанням обробки інформації;

ж) повинні відслідковуватися умови експлуатації, такі як температура і вологість, для контролю факторів, які могли б негативно вплинути на роботу обладнання обробки інформації;

з) повинен бути забезпечений захист від блискавок для всіх будівель і повинні бути встановлені пристрої захисту від перенапруги на всіх вхідних силових і комунікаційних лініях;

и) повинна бути розглянута можливість застосування спеціальних заходів захисту, таких як клавіатурні мембрани, для обладнання, що працює в виробничих умовах;

к) для обладнання, що обробляє конфіденційну інформацію, повинен бути передбачений захист, який знижує ризик витоку інформації через електромагнітне випромінювання.

2) Допоміжні комунальні служби. Обладнання має бути захищено від аварійних відімкнень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення.

Допоміжні служби (наприклад, енергопостачання, телекомунікації, водо- та газопостачання, каналізації, вентиляції і кондиціонування) повинні:

а) відповідати вимогам постачальника обладнання та місцевим законодавчим вимогам;

б) регулярно оцінюватися з точки зору їх здатності відповідати розвитку бізнесу і взаємодії з іншими службами забезпечення;

в) регулярно перевірятися для гарантії їх належного функціонування;

г) у разі необхідності, мати сигналізацію про несправності;

д) у разі необхідності, мати кілька дистанційно розділених ліній подачі.

Конституція, Цивільний кодекс, Кримінальний кодекс, Закон про охорону інформації та законодавство захисту даних окремих областей, Кодекс соціальної безпеки, Комерційний кодекс, Закон про персональні данні, Закон про авторське право, Закон про патенти та ін.

Приклади відповідних нормативів:

Адміністративні нормативи, укази і правила використання.

Приклади контрактів:

Контракти з обслуговування в області обробки даних, контракти з безпеки, що регулюють комерційні / промислові таємниці.

Питання:

Втрата конфіденційності

Чи вимагається законом забезпечувати конфіденційність даних?

Чи здатне розголошення інформації спричинити за собою кримінальну відповідальність або відшкодування збитків?

Чи є контракти, які включають підтримку конфіденційності важливої інформації?

Втрата цілісності

Чи вимагається законом забезпечувати цілісність даних?

Наскільки втрата цілісності порушить закони та нормативи?

Втрата доступності

Чи призведе збій ІТ-додатку до порушення будь-яких нормативів або навіть законів? Якщо так, то в якій мірі?

Чи повинна певна інформація бути доступна в будь-який час за законом?

Чи повинні встановлюватися кінцеві терміни, яких необхідно дотримуватися при використанні ІТ-програми?

Чи є які-небудь умови контракту для певних кінцевих термінів, які слід дотримуватися?

Сценарій пошкодження «Зниження права на інформаційне самовизначення»

При впровадженні та роботі ІТ-систем і додатків існує ризик порушення інформаційного самовизначення або навіть зловживання особистими даними.

Приклади порушення права інформаційного самовизначення:

– заборонений збір особистих даних без законної на це підстави або згоди людини;

– заборонений збір інформації під час обробки або передачі особистих даних;

– заборонене розголошення особистих даних;

– заборонене використання особистих даних для цілей, відмінних від тих, для яких вони збиралися;

– заборонене пошкодження особистих даних в ІТ-системах або під час передачі даних.

Наступні питання може використовуватися для оцінки наслідків і розмірів будь-яких порушень:

Питання:

Втрата конфіденційності

Яких збитків може бути завдано людині, якщо не дотримана конфіденційність особистих даних?

Чи обробляються будь-які особисті дані із забороненою метою?

Чи можлива обробка особистих даних із поважної причини, наприклад, у зв'язку зі здоров'ям людини або економічною ситуацією?

Які втрати або пошкодження можуть виникнути через зловживання збереженням особистих даних?

Втрата цілісності

Яких збитків може бути завдано людині, якщо особисті дані випадково спотворені (пошкоджені) або навмисне підроблені?

Коли втрата цілісності особистих даних може бути вперше помічена?

Втрата доступності

Якщо в ІТ-додатку стався збій, або особисті дані були втрачені або навіть підроблені під час проблемної передачі даних, чи можливо, що така людина зазнає негативний вплив на своє соціальне становище або особисті чи економічні незручності?

Сценарій пошкодження «Фізичні пошкодження»

Несправна робота ІТ-системи або ІТ-додатку може призвести до нещасного випадку, недієздатності або навіть смерті. Розмір пошкодження повинен бути оцінений на основі пошкодження людини.

Приклади таких ІТ-додатків і систем:

– Комп'ютери медичного контролю;

– Системи медичного діагностування;

– Комп'ютери контролю польотів;

льовано від засобів оброблення інформації точки доступу, такі як зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не санкціоновано, можуть увійти до службових приміщень.

Повинні бути враховані наступні рекомендації:

а) доступ до зони доставки та відвантаження з зовнішньої сторони будівлі повинен бути обмежений ідентифікованим і ті, що мають дозвіл персоналом;

б) зона доставки і відвантаження повинна бути сформована так, щоб прийом і відправка могли бути здійснені без доступу кур'єра до інших частин будівлі;

в) зовнішні двері зони доставки та відвантаження повинні бути закриті в той час, коли внутрішні відкриті;

г) отримані матеріали повинні бути оглянуті та перевірені на наявність вибухових речовин, хімікатів та інших небезпечних матеріалів до того, як будуть переміщені із зони доставки та відвантаження;

д) отримані матеріали повинні бути зареєстровані на вході відповідно до процедур управління активами;

е) посилки, що одержуються та відправляються, повинні бути фізично відокремлені один від одного, якщо це можливо;

ж) отримані матеріали повинні бути оглянуті на предмет наявності слідів відкриття у дорозі. Якщо такі свідоцтва виявлені, необхідно негайно повідомити співробітникам служби безпеки.

Обладнання.

Ціль: Запобігти втратам, пошкодженню, крадіжці або компрометації ресурсів СМІБ та перериванню діяльності організації.

1) Розміщення та захист обладнання. Обладнання має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу.

Для захисту обладнання повинні бути прийняті до уваги наступні рекомендації:

а) обладнання повинно бути розміщено так, щоб звести до мінімуму вхід у робочу зону без необхідності;

б) обладнання, яке обробляє інформацію та оперує критично важливими даними, повинна розміщуватись таким чином, щоб знизити ризик того, що особи, які не мають дозволи, побачать інформацію в процесі її обробки;

ПАМ'ЯТКА щодо забезпечення режиму безпеки та експлуатації обладнання встановленого в приміщенні, що підлягає захисту № _____

Відповідальність за режим безпеки в приміщенні, що підлягає захисту (ЗП) і правильність використання встановлених у ньому технічних засобів несе особа, яка постійно в ньому працює, або особа, спеціально на те уповноважена. Установка нового обладнання, меблів тощо або заміна їх, а також ремонт приміщення повинні проводитися тільки за погодженням з підрозділом (фахівцем) щодо ЗІ підприємства. У неробочий час приміщення повинно замикатися на ключ. У робочий час, у разі відсутності керівника, приміщення повинно замикатися на ключ або залишатися на відповідальності осіб, призначених керівником підрозділу. При проведенні конфіденційних заходів побутова радіоапаратура, встановлена в приміщенні (телевізори, радіоприймачі тощо), повинна відключатися від мережі електроживлення. Повинні бути виконані приписи на експлуатацію засобів зв'язку, обчислювальної техніки, оргтехніки, побутових приладів та ін. обладнання, встановленого в приміщенні. Забороняється використання в ЗП радіотелефонів, кінцевих пристроїв стільникового, пейджингового та транкінгового зв'язку. При установці в ЗП телефонних і факсимільних апаратів з автовідповідачем, спікерфоном і пристроїв, які мають вихід в міську АТС, слід відключати ці апарати на час проведення конфіденційних заходів. Повсякденний контроль за виконанням вимог із захисту приміщення здійснюють особи, відповідальні за приміщення, і служба безпеки підприємства.

Періодичний контроль ефективності заходів захисту приміщення здійснюється фахівцями із ЗІ.

Примітка: У пам'ятку доцільно включати і інші відомості, що враховують особливості встановленого в ЗП обладнання; дії персоналу в разі спрацювання встановленої в приміщенні сигналізації, порядок увімкнення засобів захисту, організаційні заходи захисту і т.і.

Перелік обладнання, встановленого в приміщенні.

Вид обладнання, Тип, Обліковий, Номер (зав.), Дата установки. Клас ТЗ, Відомості по сертифікації.

6) Зони доставки та відвантаження. Щоб уникнути несанкціонованого доступу, має бути контрольовано й, за можливості, ізо-

– Системи маршрутизації руху транспорту.

Питання:

Втрата конфіденційності

Чи може людина отримати фізичну або психологічну травму через розголошення особистих даних?

Втрата цілісності

Чи може втручання в послідовність програм або даних наразити на небезпеку здоров'я людей?

Втрата доступності

Чи може збій ІТ-додатку або системи безпосередньо загрожувати здоров'ю людей?

Сценарій пошкодження «Порушення виконання обов'язків»

Саме втрата доступності ІТ-додатку або цілісності даних може значно вплинути на можливість компанії або держустанови виконувати свої завдання. У такому контексті, серйозність будь-якого збитку залежить від тривалості пошкодження і ступеня, до якої обмежені надані послуги.

Приклади:

– недотримання кінцевих термінів у зв'язку зі затримками в обробці адміністративних процедур;

– поставка із запізненням у зв'язку зі затримкою обробки замовлень;

– неякісна продукція через невірні параметри контролю;

– недостатня перевірка якості у зв'язку зі збоями системи тестування.

Питання:

Втрата конфіденційності

Чи є дані для яких критична конфіденційність при виконанні завдання (наприклад, Інформація про судове переслідування, рішення розслідування)?

Втрата цілісності

Чи можуть зміни даних обмежити виконання завдань так, що організація не зможе працювати?

Чи буде задана значна шкода, якщо завдання виконувалися з використанням «перекручених» (неперевірених, неправильних / неправдивих) даних? Коли були вперше помічені заборонені зміни даних?

Чи можуть спотворені дані розглянутих ІТ-додатків привести до помилок в інших ІТ-додатках?

Якщо дані були неправильно присвоєні людині, яка насправді їх не створювала, які можуть бути наслідки?

Втрата доступності

Чи може збій ІТ-додатку настільки серйозно вплинути на роботу організації, що простої більше неприпустимі?

Чи будуть якісь інші ІТ-додатки порушені при збої даного ІТ-додатку?

Чи важливо для організації, щоб доступ до ІТ-додатків, включаючи програми і дані, був забезпечений в будь-який час?

Сценарій пошкодження «Негативний внутрішній або зовнішній вплив»

Різні негативні внутрішні і зовнішні впливи можуть бути викликані втратою однієї з трьох основних цінностей: конфіденційності, цілісності або доступності, наприклад:

– Компрометація репутації організації;
– Втрата довіри в організації;
– Втрата трудової дисципліни;
– Погіршення комерційних відносин між компаніями партнерами;
– Втрата довіри до якості робіт організації;
– Втрата конкурентоспроможності.

Рівень ушкоджень залежить від серйозності втрати довіри або ступеня поширення внутрішнього або зовнішнього впливу.

Таке пошкодження може мати багато причин:

– нездатність організації діяти при збої ІТ-системи;
– невірні публікації у зв’язку з підтасування даних;
– неправильне розміщення замовлень у зв’язку з пошкодженням програми контролю запасів;
– недотримання угод конфіденційності;
– звинувачення не тих людей;
– один відділ не здатний виконати свої обов'язки у зв’язку з помилками на інших ділянках;
– передача «списку розшукуваних» зацікавленим третім особам;
– витік конфіденційних даних в пресу.

4) Захист від зовнішніх та інфраструктурних загроз. Має бути розроблено й застосовано фізичний захист від пошкодження внаслідок природних катаклізмів, акцій громадської непокори та аварій.

Слід проконсультуватися з фахівцем, яким чином уникнути пошкоджень від пожежі, повені, землетруси, вибуху, громадських заворушень та інших форм загроз природного, техногенного або соціального характеру.

Керівні документи:

Кодекс цивільного захисту України, (Відомості Верховної Ради (ВВР), 2013, № 34-35, ст.458).

Правила пожежної безпеки в Україні. Затверджено Наказ Міністерства внутрішніх справ України 30.12.2014 № 1417. Зареєстровано в Міністерстві юстиції України 05 березня 2015 р. за № 252/26697.

5) Робота в зонах безпеки. Має бути розроблено та застосовано процедури роботи в зонах безпеки.

Повинні бути враховані наступні рекомендації:

а) про існування зони, що охороняється або діяльності в ній повинен знати тільки той персонал, якому це належить знати в силу службових обов'язків;

б) в охоронних зонах для забезпечення безпеки і запобігання зловмисних дій повинна бути виключена робота без супроводу;

в) безлюдні охоронні зони повинні бути фізично закриті і періодично оглядатися;

г) фото-, відео-, аудіо- та інша апаратура, що записує, така як камери в мобільних пристроях, повинні бути заборонені без спеціального дозволу.

Заходи з роботи в охоронюваних зонах включають в себе заходи для співробітників і зовнішніх користувачів, що працюють в зоні, що охороняється, і охоплюють всі види діяльності, які здійснюються в цій зоні.

Приклад: ТЕХНІЧНИЙ ПАСПОРТ
на приміщення, що підлягає захисту № _____

Склав *Підпис спеціаліста підрозділу із захисту інформації*

Ознайомлений *Підпис особи, відповідальної за приміщення*

надзвичайній ситуації. Ідентичність відвідувачів повинна бути встановлена відповідними методами;

б) доступ в зони, де обробляється або зберігається конфіденційна інформація, повинен бути обмежений тільки авторизованими відвідувачами застосуванням відповідних засобів контролю проходу, наприклад, використанням механізму ідентифікації за двома ознаками, таким як картка доступу і секретний PIN-код;

в) повинен надійним чином вестися і перевірятися рукописний або електронний журнал всіх відвідувань;

г) всі співробітники і працюючи за контрактом, в також відвідувачі зобов'язані носити певні знаки візуальної ідентифікації і повинні негайно повідомляти в службу безпеки, якщо зустріли відвідувачів без супроводу і кого-то без знаку візуальної ідентифікації;

д) персонал зовнішніх служб забезпечення тільки в разі потреби повинен мати обмежений доступ до охоронюваних зон або обладнання, що обробляє конфіденційну інформацію, цей доступ повинен бути авторизований і контрольований;

е) права доступу до охоронюваних зон повинні регулярно переглядатися і оновлюватися, а також скасовуватися в разі необхідності.

3) Забезпечення безпеки офісів, кімнат та обладнання. Має бути розроблено й застосовано фізичну безпеку офісів, кімнат та обладнання.

Для захисту офісів, приміщень і обладнання повинні бути прийняті до уваги наступні рекомендації:

а) критично важливе обладнання повинно бути розміщено так, щоб виключити відкритий доступ;

б) там, де це може бути застосовано, будівлі повинні бути непомітними і давати мінімум інформації про своє призначення, без явних ознак – зовні або всередині будівлі – що дозволяють зробити висновок про наявність діяльності з оброблення інформації;

в) обладнання повинно бути налаштоване таким чином, щоб конфіденційна інформація або дії не були видимі і чутні зовні. При необхідності, має бути передбачено електромагнітне екранування;

г) довідники та внутрішні телефонні книги, що містять інформацію про розміщення устаткування, що обробляє інформацію, не повинні бути легко доступні для неавторизованих осіб.

Питання:

Втрата конфіденційності

Яке значення для організації матиме невирішена публікація важливих даних, що зберігаються в IT-додатку?

Чи може втрата конфіденційності збережених даних викликати ослаблення конкурентоспроможності?

Чи може розголошення конфіденційних даних викликати сумніви в дотриманні службової таємниці?

Чи може публікація даних призвести до політичної або соціальної уразливості?

Чи можуть співробітники втратити довіру до організації через недозволену публікацію даних?

Втрата цілісності

Яких збитків може бути завдано через обробку, розповсюдження або передачу некоректних або неповних даних?

Чи стане загальновідомим підробка даних?

Чи може публікація «перекручених» даних призвести до втрати престижу?

Чи може публікація «перекручених» даних призвести до політичної або соціальної уразливості?

Чи можуть спотворені дані призвести до зниження якості продукції і, як наслідок, до втрати престижу?

Втрата доступності

Чи обмежить збій в IT-додатку інформаційні послуги, які надаються зовнішнім організаціям?

Чи перешкоджає збій IT-додатків досягненню цілей організації?

Коли збій IT-додатку стає помітним зовні?

Сценарій пошкоджень «Фінансові наслідки»

Прямий або непрямий фінансовий збиток може виникнути через втрату конфіденційності даних, які вимагають захисту, змін в даних або збою IT-додатку. Приклади:

– недозволене оприлюднення науково-дослідних результатів;

– махінації з фінансовими даними в системах обліку;

– збій в IT – контрольованої промислової системі, що призводить до зниження продажів;

– отримання інформації за маркетинговою стратегією або даними товарообігу;

– збій системи бронювання в туристичному агентстві;
– збій на сервері електронної торгівлі;
– збій банківських платіжних транзакцій;
– злодійство або знищення апаратури.

Загальний рівень пошкоджень складається з витрат, понесених безпосередньо або побічно, наприклад, через пошкодження власності, а також претензій за збитки і додаткових витрат (наприклад, на відновлення).

Питання:

Втрата конфіденційності

Чи може публікація конфіденційних даних призвести до вимог відшкодування збитків?

Чи є в ІТ-додатках дані, які можуть забезпечити фінансові вигоди третім особам, якщо вони потраплять до них (наприклад, Конкурентам)?

Чи є дані досліджень збережені за допомогою ІТ-додатків, які мають значну цінність? Що станеться, якщо такі дані скопіюють і передадуть без дозволу?

Чи може якесь ушкодження бути викликано передчасної публікацією важливих даних?

Втрата цілісності

Чи можуть будь-які дані, що стосуються обліку, змінюватися через маніпулювання даними, спрямованого на створення фінансових втрат?

Чи може розголошення невірної інформації призвести до вимог відшкодування збитків?

Чи може порушений порядок даних призвести до фінансових втрат (наприклад, для випуску продукції точно до заданого терміну)?

Чи можуть пошкоджені дані призвести до неправильних бізнес-рішень?

Втрата доступності

Чи може завдати шкоди збій ІТ-додатку продукції, управлінню запасами або поширенню?

Якщо в ІТ-додатку відбувається збій, чи будуть фінансові втрати через скасування платежів або втрати відсотків?

стінами, щоб забезпечити необхідний рівень захищеності відповідно до діючих регіональних, національних та міжнародних стандартів. Вони повинні безвідмовно функціонувати відповідно до місцевих правил пожежної безпеки;

е) повинні бути встановлені відповідні системи виявлення проникнення, відповідні регіональним, національним або міжнародним стандартам, та регулярно перевірятися на предмет того, що ними охоплені всі зовнішні двері і доступні вікна. Невикористовувані площі повинні бути оснащені постійно працюючою сигналізацією. Захист також повинен бути забезпечений і для інших зон, наприклад, комп'ютерного залу або серверних;

ж) обладнання обробки інформації, що знаходиться під контролем організації, повинно бути відокремлене від устаткування, керованого зовнішніми сторонами.

Фізичний захист може бути забезпечена введенням однієї або декількох ліній захисту навколо приміщень організації та пристроїв обробки інформації. Застосування множинних ліній захисту дає додатковий захист, так як збій на одній не веде до того, що безпека буде негайно порушена.

Зоною, що охороняється може бути офіс, що замикається або кілька приміщень, оточених безперервної внутрішньої лінією захисту. Можуть бути необхідні додаткові лінії захисту і периметри для контролю фізичного доступу між зонами з різними вимогами щодо безпеки всередині периметра безпеки. Особливу увагу до безпечного фізичного доступу має бути приділено в тому випадку, коли в будівлі розміщуються активи багатьох організацій.

Застосування заходів фізичного контролю, особливо для охоронюваних зон, повинно бути пов'язане з технічними та економічними обставинами організації, як це випливає з оцінки ризиків.

2) Заходи безпеки фізичного прибуття. Зони безпеки має бути захищено належними заходами безпеки прибуття, щоб гарантувати, що доступ дозволений лише персоналу, який отримав санкцію:

а) дата і час приходу і відходу відвідувачів має реєструватися, а також відвідувачі повинні супроводжуватися, якщо тільки їх прихід ні заздалегідь узгоджений. Їм повинен бути наданий прохід тільки для конкретних і схвалених цілей, вони повинні бути проінструктовані за вимогами безпеки даної зони і процедурам дій у

процедури для роботи з юридичними запитами на доступ до криптографічних ключів, наприклад, зашифрована інформація може бути затребувана для розшифрування і використання в якості свідоцтва у суді [1, 2].

4.7. Системи фізичної безпека

Зони безпеки.

Ціль: Запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в її інформацію та засоби оброблення інформації.

1) Периметр фізичної безпеки. Для захисту зон, що містять конфіденційну або критичну інформацію чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки.

При формуванні фізичних периметрів безпеки повинні бути прийняті до уваги і виконані, де це можливо, такі рекомендації:

а) периметри безпеки повинні бути визначені, а розташування і ступінь захисту, що забезпечується периметрами, повинен залежати від вимог з безпеки активів всередині периметра і результатів оцінки ризиків;

б) периметри будівель і місць знаходження пристроїв обробки інформації повинні бути фізично міцними (тобто не повинні мати в периметрі розривів або зон, де він може бути легко подоланий); зовнішнє перекриття, стіни та підлога повинні мати монолітну конструкцію, а всі зовнішні двері повинні бути відповідним чином захищені від несанкціонованого доступу охоронними засобами (наприклад, засуви, сигналізація, замки). Двері і вікна повинні бути закриті, поки приміщення знаходиться без нагляду, а зовнішній захист повинен включати і вікна, особливо, на першому поверсі;

в) повинні функціонувати обслуговуючи зони прийому або інші засоби контролю фізичного доступу до певних місць і будівель; доступ до певних місць і будівель повинен бути обмежений і дозволений лише авторизованому персоналу;

г) повинні бути збудовані, де це можливо, фізичні перешкоди для захисту від неавторизованого фізичного доступу і зовнішнього забруднення;

д) всі пожежні виходи по периметру повинні бути оснащені сигналізацією, бути під наглядом і перевірені в місцях з'єднання зі

Скільки буде коштувати виправити або відновити ІТ-систему, якщо в ній стався збій, вона була зруйнована або вкрадена?

Чи може збій ІТ-додатку призвести до неплатоспроможності або до договірних неустойках?

На скількох важливих клієнтів вплине збій ІТ-програми?

Крок 3: Реєстрація результатів

Рекомендується, щоб вимоги безпеки, визначені вище, для різних ІТ-додатків записувалися в таблицю. Такий централізований документ надає можливість використовувати його під час подальшого визначення вимог безпеки для ІТ-систем.

Тут необхідно подбати про те, щоб забезпечити реєстрування не тільки оцінені вимоги безпеки, а й ті які лежать в основі обґрунтування цих висновків. Ці обґрунтування забезпечать те, що висновки можна відстежувати і використовувати повторно в подальшому [4].

Приклад:

Bundesamt für Organisation und Verwaltung (Федеральна служба організації та адміністрування, Federal Agency for Organisation and Administration, BOV).

У наведеній нижче таблиці 2.5, відображено основні ІТ-додатки, їх вимоги безпеки і обґрунтування призначень категорій вимог безпеки.

Таблиця 2.5. Основні ІТ-додатки, їх вимоги безпеки і обґрунтування призначень категорій вимог безпеки

ІТ-додаток			**Оцінка вимог безпеки**		
1	2	3	4	5	6
No	**Назва**	**Перс. данні**	**Основний параметр**	**Вимоги безпеки**	**Обґрунтування**
A1	Обробка даних персоналу	X	Конфіденційність	Високі	Дані про персонал становлять особливо важливі деталі, розкриття яких може значно зашкодити відповідній людині
			Цілісність	Нормальні	Вимоги до захисту нормальні, тому що помилки швидко виявляють, і дані можуть бути виправлені пізніше
			Доступність	Нормальні	Простої до тижня можуть керуватися вручну

Закінчення табл. 2.5

1	2	3	4	5	6
A2	Обробка переваг	X	Конфіденційність	Високі	Дані про вигоди включають персональні дані, у яких особливо високі вимоги захисту. Деякі з них можуть мати відношення до хвороб і результатів мед. аналізів. Розголошення цих даних може бути дуже шкідливим для відповідних людей
			Цілісність	Нормальні	Вимоги до захисту нормальні, тому що помилки швидко виявляють, і дані можуть бути виправлені пізніше
			Доступність	Нормальні	Простої до тижня можуть керуватися вручну

Також доцільно подивитися за межі згаданої інформації і розглянути вимоги безпеки ще із загальної точки зору на бізнес-процеси або завдання фахівців. Це необхідно для опису цілей IT-додатків у бізнес-процесі або завдання фахівця, і з цього слід встановити їх важливість. Ступінь важливості може бути класифікована таким чином – важливість IT-додатків для бізнес-процесу або завдання фахівця:

– **Нормальна**: бізнес-процес або завдання фахівця можуть виконуватися альтернативними засобами (наприклад, вручну) з прийнятним рівнем додаткових витрат;

– **Висока**: бізнес-процес або завдання фахівця можуть виконуватися альтернативними засобами (наприклад, вручну) зі значними додатковими витратами;

– **Дуже висока**: бізнес-процес або завдання фахівця взагалі не можуть виконуватися без IT-додатків.

Перевага прийняття таких докладних розподілів у тому, що керівництво може регулювати вимоги безпеки для окремих IT-додатків при визначенні вимог захисту. Наприклад, може бути, що відповідальний за IT-додаток бачить його вимоги безпеки як «нормальні», тоді як керівник оцінив би його більш високо, висловивши

в) розподілу ключів тим, кому вони призначені, включаючи і те, як вони повинні бути активовані після отримання;

г) зберігання ключів, включаючи те, як авторизовані користувачі будуть отримувати доступ до ключів;

д) зміни або оновлення ключів, в тому числі і правила, що визначають, коли ключі повинні бути змінені і як це повинно бути зроблено;

е) дій з скомпрометованими ключами;

ж) анулювання ключів, включаючи те, як ключ повинен бути анульований або деактивований, наприклад, коли ключі були скомпрометовані або коли користувач залишає організацію (в цьому випадку ключі повинні бути архівовані);

з) відновлення втрачених або пошкоджених ключів;

и) резервного копіювання або архівування ключів;

к) знищення ключів;

л) реєстрації та аудиту діяльності, пов'язаної з управліннями ключами.

Для того, щоб зменшити ймовірність невідповідного використання повинні бути визначені дати активації і деактивації ключів так, щоб ключі могли бути використані тільки в період, визначений у відповідній політиці управління ключами.

Крім того, для більш надійного управління таємними і персональними ключами повинна перевірятися справжність відкритих ключів. Процес автентифікації може бути виконаний за допомогою сертифікатів відкритих ключів, які, зазвичай, випускаються центром сертифікації, який повинен бути визнаною організацією з відповідними реалізованими засобами управління і процедурами для забезпечення необхідного рівня довіри.

Угоди про рівень обслуговування або контракти із зовнішніми постачальниками криптографічних послуг, наприклад, центрами сертифікації, повинні включати в себе питання відповідальності, надійності послуг і часу відгуку при наданні послуги.

Управління криптографічними ключами є принципово важливим з точки зору результативного використання криптографічних методів. Стандарт ISO / IEC 11770 містить детальну інформацію з управління ключами.

Криптографічні методи також можуть бути використані для захисту криптографічних ключів. Можливо, можуть знадобитися

цілісності збереженої або переданої уразливої або важливої інформації;

в) незаперечність: використання криптографічних методів для забезпечення свідоцтва настання або відсутністю події або дії;

г) автентифікація: використання криптографічних методів для автентифікації користувачів і інших компонентів системи, що запитують доступ до користувачів системи, компонентів і ресурсів або взаємодіючих з ними.

Формування уявлення, наскільки підходить те чи інше криптографічне рішення, має розглядатися як частина ширшого процесу оцінки ризику і вибору засобів реалізації. Така оцінка може потім бути використана для визначення, чи є криптографічний метод прийнятним, який різновид методу повинен бути застосований, для яких цілей і якого бізнес-процесу.

Політика використання криптографічних методів необхідна для досягнення максимальної вигоди і мінімізації ризиків використання криптографічних методів, а також щоб уникнути неналежного або неправильного використання.

Необхідно звернутися за порадою до фахівця у виборі відповідних криптографічних методів для досягнення цілей політики ІБ.

2) Управління ключами. Має бути розроблено та впроваджено політику використання, захисту й часу життя криптографічних ключів для всього їх життєвого циклу.

Політика повинна містити вимоги до управління криптографічними ключами протягом усього їх життєвого циклу, включаючи генерацію, зберігання, архівування, відновлення, розподіл, анулювання та знищення ключів.

Всі криптографічні ключі повинні бути захищені від модифікації або втрати. Крім цього, секретні і персональні ключі вимагають захисту від несанкціонованого використання, так само як і від розкриття. Устаткування, що застосовується для генерації, зберігання та архівування ключів повинно бути фізично захищене.

Система управління ключами повинна базуватися на узгодженому комплексі стандартів, процедур і методів забезпечення безпеки для:

а) генерації ключів для різних криптографічних систем і додатків;

б) випуску і отримання сертифікатів відкритого ключа;

свою думку про програму в межах більш широкого бізнес-процесу або завдання фахівця.

Ці додаткові дані також слід записати в таблицю.

Виконання:

– Визначення категорій «нормальних», «високих» і «дуже високих» вимог безпеки, або адаптація їх до організації;

– Визначення вимог безпеки для зареєстрованих ІТ-додатків, використовуючи сценарії пошкоджень і списки питань;

– Документування вимог безпеки ІТ-додатків і їх відносин в таблиці.

Визначення вимог безпеки для ІТ-систем

Щоб визначити вимоги захисту для ІТ-системи, спочатку повинні бути розглянуті ІТ-додатки, які безпосередньо пов'язані з ІТ-системою. Визначення, найбільш важливих ІТ-додатків, було реалізовано на попередньому кроці «Документування інформації про ІТ-додатки та відповідні положення про інформацію, що з ними пов'язана».

Щоб визначити вимоги безпеки ІТ-системи, слід в цілому розглянути потенційний збиток відповідним ІТ-додаткам. Збиток або повне руйнування з найбільш серйозним впливом визначає вимоги безпеки ІТ-системи (**принцип максимуму**).

У процесі вивчення можливого збитку і його наслідків, має бути зрозуміло, що ІТ-додатки ІТ-системи можуть використовувати результати інших ІТ-додатків як свої вхідні дані. Очевидно, менш важливий ІТ-додаток А може стати значно важливішим, якщо інший, важливий, ІТ-додаток В залежить від результатів А. В цьому випадку вимоги безпеки, визначені для ІТ-додатка В, повинні також поширюватися на ІТ-додаток А. Якщо ці ІТ-додатки знаходяться в різних ІТ-системах, то вимоги безпеки однієї ІТ-системи повинні поширюватися на іншу (**дотримання залежностей**).

Якщо кілька ІТ-додатків або інформація про ІТ-систему обробляються і накопичуються, шкідливі події в одній ІТ-системі призводять до великого спільного пошкодження. В цьому випадку, вимоги безпеки ІТ-системи відповідно підвищуються (**сукупний ефект**).

Приклад: усі ІТ-додатки, необхідні для запису даних клієнта, знаходяться на одному мережевому сервері. Шкода в разі збою цих

ІТ-додатків буде оцінена як низька, проте є альтернативи. Так, якщо відбудеться збій на сервері (і тому також на всіх ІТ-додатках), загальний збиток буде значно більший. Організація може бути не в змозі далі виконувати свою роль у таких обставинах. Тому вимоги безпеки цих «центральних» компонент також повинні бути вищими.

Протилежний ефект теж можливий. Тому для ІТ-додатка можливо мати високі вимоги безпеки, але його вимоги безпеки не поширюватимуться на розглянуту ІТ-систему, тому що тільки незначна частина ІТ-додатка працює в цій ІТ-системі (**ефект поширення**).

Приклади: Ефект поширення переважно виникає для забезпечення доступності основних цінностей. Тому, наприклад, там, де ІТ-системи розроблені надлишковим чином, вимоги безпеки окремих компонент можуть бути нижчими, ніж для всього додатка. Ефект поширення також можливий для конфіденційності. Якщо можна гарантувати, що клієнт отримує тільки некритичні дані з високо конфіденційного додатку бази даних, клієнт, на відміну від сервера бази даних, має лише низькі вимоги безпеки.

Надання результатів

Результати оцінки вимог безпеки ІТ-систем повинні послідовно зберігатися в таблиці. Тут також доцільно перераховувати вимоги безпеки, які кожна ІТ-система має відносно конфіденційності, цілісності та доступності. Загальні вимоги безпеки для ІТ-системи, у свою чергу, отримують з максимальних вимог безпеки до трьох основних цінностей: конфіденційності, цілісності та доступності.

Тому ІТ-система має високі загальні вимоги безпеки, якщо одна з основних цінностей має «високу» вимогу до захисту. Але взагалі доцільно записувати вимоги безпеки ІТ-системи для всіх трьох основних цінностей, оскільки зазвичай із них розробляють різні типи заходів безпеки.

Для ІТ-системи, наприклад, загальні вимоги безпеки можуть бути високими, тому що вимоги безпеки для конфіденційності високі, але нормальні для цілісності та доступності. Тому хоча загальні вимоги безпеки високі, мається на увазі, що в результаті вимоги безпеки для цілісності та доступності повинні бути підвищені. Не потрібно ніяких додаткових заходів для захисту цілісності та доступності.

1) Політика використання криптографічних засобів. Має бути розроблено та впроваджено політику використання криптографічних засобів для захисту інформації.

При розробці політики в області криптографії слід врахувати наступне:

а) підхід до управління застосуванням криптографічних методів в рамках всієї організації, включаючи загальні принципи, на яких повинен бути заснований захист бізнес-інформації;

б) повинен бути визначений, ґрунтуючись на оцінці ризиків, необхідний рівень захисту з урахуванням типу, стійкості і якості необхідного криптографічного алгоритму;

в) використання шифрування для ЗІ при передачі через мобільні, знімні носії або за допомогою ліній зв'язку;

г) підхід до управління ключами, включаючи методи захисту криптографічних ключів та відновлення зашифрованої інформації в разі втрати, компрометації або пошкодження ключів;

д) ролі та обов'язки, наприклад, хто відповідає за:

1) реалізацію політики;

2) управління ключами, включаючи їх генерацію;

е) стандарти, які повинні бути прийняті в цілях результативного застосування в рамках всієї організації (яке рішення для якого бізнес-процесу використовується);

ж) вплив застосування шифрування інформації на інструменти, які пов'язані з контролем змісту (наприклад, виявлення шкідливого коду).

При реалізації криптографічної політики організації необхідно враховувати регламенти та вимоги національних органів, які можуть бути застосовані в області використання криптографічних методів в різних країнах, а також проблеми транскордонної передачі шифрованого інформації.

Криптографічні методи можуть бути використані для досягнення різних цілей, пов'язаних із ЗІ, наприклад:

а) конфіденційність: використання шифрування для захисту уразливої або важливої інформації, що зберігається або передається;

б) цілісність/справжність: використання цифрових підписів або кодів автентичності повідомлення для перевірки автентичності або

б) вихідні коди і бібліотеки вихідних кодів повинні управлятися відповідно до встановлених процедур;

в) персонал технічної підтримки не повинен мати необмежений доступ до бібліотек вихідних кодів;

г) оновлення бібліотек вихідних кодів і пов'язаних з ними елементів, а також видача вихідного коду програмістам має виконуватися тільки після проходження відповідної авторизації;

д) лістинги програм повинні зберігатися у безпечному середовищі;

е) повинні зберігатися записи всіх звернень до бібліотек вихідних кодів;

ж) обслуговування та копіювання бібліотек вихідних кодів повинне проводитися за суворими процедурами контролю змін.

Якщо вихідний код програми передбачається публікувати, то повинні бути прийняті до уваги додаткові заходи контролю для гарантії його цілісності (наприклад, цифровий підпис) [1, 2].

4.6. Криптографічне забезпечення

Тайнопис

Відправник і одержувач використовують перетворення, відомі тільки їм двом. Стороннім особам невідомий сам алгоритм шифрування. Деякі фахівці вважають, що тайнопис не є криптографією взагалі.

Криптографія з ключем. Алгоритм впливу на дані, що передаються, відомий всім стороннім особам, але він залежить від деякого параметра – «ключа», яким володіють тільки відправник і одержувач.

Симетричні криптоалгоритми. Для кодування і розшифровки повідомлення використовується один і той же блок інформації (ключ).

Асиметричні криптоалгоритми. Алгоритм – для кодування повідомлення використовується один («відкритий») ключ, відомий всім бажаючим, а для розшифровки – інший («закритий»), що існує тільки в одержувача.

Криптографічні засоби захисту

Ціль: Гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності.

Особлива важливість надається наданню пояснень зробленим оцінкам, щоб вони були зрозумілі третім особам. У такому випадку можна робити посилання на оцінку вимог безпеки для IT-додатків.

Приклад:

Bundesamt für Organisation und Verwaltung (Федеральна служба організації та адміністрування, Federal Agency for Organisation and Administration, BOV).

Може бути створена наступна таблиця 2.6.

Зауваження: Якщо більшість IT-додатків в системі мають тільки нормальні вимоги безпеки і тільки один або кілька мають вимоги безпеки високі, то треба розглянути, чи варто експортувати їх в ізольовану IT-систему, хоча набагато простіше і доцільніше захистити такий тип системи, а також це було б дешевше. Аргументи на користь такої альтернативи можна підготувати для подання керівництву для прийняття рішення.

Таблиця 2.6. Основні IT-додатки та оцінка вимог безпеки для них

IT-система		**Оцінка вимог безпеки**		
1	2	3	4	5
No.	**Опис**	**Основний параметр**	**Вимоги безпеки**	**Обґрунтування**
S1	Сервер для відділу персоналу	Конфіденційність	Високі	Принцип максимуму
		Цілісність	Нормальні	Принцип максимуму
		Доступність	Нормальні	Принцип максимуму
S2	Primary domain controller	Конфіденційність	Нормальні	Принцип максимуму
		Цілісність	Високі	Принцип максимуму
		Доступність	Нормальні	Згідно з оцінкою вимог безпеки для програми А4, ця основна цінність може бути високою. Однак слід взяти до уваги, що цей додаток поширюється на дві комп'ютерні системи.

Закінчення табл. 2.6

1	2	3	4	5
				Також можливо автентифікувати персонал, що працює в офісі в Бонні, через резервний контролер домену в Берліні. Ненадійність первинного контролера домену прийнятна на період до 72 годин. Тому вимоги безпеки «нормальні» в результаті цього ефекту поширення.

Додаткові засоби:

Були розроблені форми в якості додаткових матеріалів для завершення визначення вимог безпеки; вони доступні з ресурсів IT-Grundschutz.

Виконання:

– оцінка вимог безпеки IT-систем, використовуючи вимоги безпеки для IT-додатків;

– розгляд залежностей, принципу максимуму і, за необхідності, сукупного ефекту і ефекту поширення;

– запис результатів по конфіденційності, цілісності і доступності, а також обґрунтування для кожної IT-системи (групи).

Визначення вимог безпеки для ліній зв'язку

Як тільки вимоги безпеки для цієї IT-системи були визначені, повинні розглядатися вимоги безпеки для конфігурації мережі. Основою для подальших обговорень знову є план мережі для розглянутих IT-ресурсів.

Щоб підготувати рішення щодо того, які маршрути комунікацій вимагають використання заходів криптографічного захисту, які частини мережі повинні мати вбудовану надмірність, на які з'єднання слід очікувати атаки інсайдерів і зовнішніх недоброзичливців, слід розглянути різні лінії зв'язку, а також самі IT-системи. У цьому аналізі слід розглядати як критичні такі лінії зв'язку:

– Лінії зв'язку із зовнішнім світом, тобто ті, які ведуть у/або через неконтрольовані області (наприклад, в Інтернет або через ділянку, до якої суспільство має доступ). Це також може бути

заходи безпеки системи та прикладних програм, має бути обмежено та суворо контрольовано.

Повинні бути враховані наступні рекомендації по використанню утиліт, які могли б обходити засоби контролю системи і застосунків:

а) використання процедур ідентифікації, автентифікації і авторизації для цих утиліт;

б) відділення утиліт від прикладного ПЗ;

в) обмеження використання утиліт мінімально можливим на практиці числом довірених, авторизованих користувачів;

г) авторизація в кожному конкретному випадку використання утиліт;

д) обмеження доступності утиліт, наприклад, в період санкціонованої зміни;

е) реєстрація всіх випадків використання утиліт;

ж) встановлення та документування рівнів авторизації для утиліт;

з) видалення або відключення всіх непотрібних утиліт;

и) не робити утиліти доступними тим користувачам, у яких є доступ до застосунків у системах, де потрібно поділ обов'язків.

На більшості комп'ютерів встановлена одна або більше утиліт, які могли б обходити засоби контролю системи і застосунків.

5) Контроль доступу до початкових кодів програм. Доступ до початкових кодів програм має бути обмежений.

Доступ до вихідного коду програм і пов'язаних з ним елементів (таким, як схеми, специфікації, плани верифікації та валідації) повинен бути строго контрольованим з метою запобігання включення в нього несанкціонованої функціональності та уникнення ненавмисних змін, так само як і для збереження конфіденційності цінної інтелектуальної власності. Відносно вихідного коду це може бути досягнуто контрольованим централізованим зберіганням такого коду, переважно в бібліотеках вихідних кодів. Наступні рекомендації повинні бути прийняті до уваги для контролю доступу до таких бібліотек вихідних кодів з метою зниження можливості внесення спотворень в комп'ютерні програми:

а) там, де це можливо, бібліотеки вихідних кодів не повинні міститися в робочих системах;

– віддалена система;
– веб-сервіси;
– поштові сервіси;
– парольний менеджер;
– локальні програми;
– архіватори;
– криптовані диски;
– флешкарти і інші пристрої;
– BIOS та ін.

Якщо паролі передаються по мережі відкритим текстом під час процедури входу, вони можуть бути перехоплені мережевими програмами аналізу трафіку (sniffers).

3) Система управління паролем. Системи для управління паролями мають бути інтерактивними і забезпечувати якісні паролі.

Система управління паролями повинна:

а) примушувати кожного користувача використовувати ідентифікаційні дані і паролі для забезпечення відстеження;

б) дозволяти користувачеві вибирати і змінювати свої власні паролі і включати процедуру підтвердження для забезпечення можливості виправлення помилок введення;

в) змушувати використовувати паролі належної якості;

г) примусово змушувати користувачів змінювати паролі в ході першої сесії;

д) примушувати регулярно або в міру необхідності міняти паролі;

е) зберігати паролі, які використовувалися і не допускати їх повторного використання;

ж) не відображати паролі, які вводяться;

з) зберігати файли з паролями окремо від даних прикладної системи;

и) зберігати і передавати дані в захищеному вигляді.

Деякі застосунки вимагають, щоб паролі користувача були призначені незалежним адміністратором, у таких випадках вищенаведені пункти б), д) і е) не застосовні. У більшості випадків паролі вибираються і змінюються користувачами.

4) Використання привілейованих системних утиліт. Використання програм утиліт, що можуть бути спроможні скасовувати

WLAN з'єднання, тому що важко запобігти громадському доступу до них. Для зовнішніх підключень існує ризик спроб проникнення в систему, яку необхідно захищати, з боку зовнішніх зловмисників або в неї можуть бути імпортовані комп'ютерні віруси чи «Троянські коні». Крім того, за допомогою таких підключень інсайдер може передати конфіденційну інформацію в зовнішній світ.

– Лінії зв'язку, по яких передається інформація, що має високі вимоги безпеки. Відповідна інформація може мати високі вимоги безпеки щодо одного або більше основних параметрів: конфіденційності, цілісності та доступності. Це з'єднання може призначатися для навмисного спотворення чи підслуховувань. Крім того, збій такого підключення може мати шкідливий вплив на працездатність значної кількості IT-ресурсів.

– Лінії зв'язку, які не можна використовувати для передачі дуже важливої інформації. У цьому випадку особливу роль має передача конфіденційної інформації. Якщо будь-які комутуючі мережеві елементи сконфігуровані невідповідним або неправильним чином, то можливо, що саме ця інформація, яка не повинна передаватися по такому з'єднанню, все ж буде передана й у результаті стане уразливою для атак.

Підхід до збору інформації про критичні лінії зв'язку може бути наступним. Насамперед усі «зовнішні підключення» визначаються і реєструються як критичні підключення. Потім реєструються всі лінії, які використовуються IT-системами, з високими або дуже високими вимогами безпеки. Таким же чином визначається підключення, по якому передається інформація з високими вимогами безпеки. Потім вивчаються підключення, що використовуються для передачі цих дуже важливих даних. Нарешті, визначаються лінії зв'язку, по яких така інформація не повинна передаватися. Зібрана інформація повинні містити:

Маршрути зв'язку:

– чи має підключення зовнішні лінії;

– чи є інформація, що має високі вимоги безпеки, і чи відносяться вимоги безпеки до конфіденційності, цілісності або доступності;

– чи повинна інформація, що має високі вимоги безпеки, передаватися по цих лініях.

Зібрані дані можуть бути або записані в табличній формі (див. табл. 2.7), або графічно виділені на плані мережі.

Приклад:

Bundesamt für Organisation und Verwaltung (Федеральна служба організації та адміністрування, Federal Agency for Organisation and Administration, BOV).

У нашому вигаданому прикладі BOC є такі критичні з'єднання, які пояснюються в заголовках колонок таблиці 2.7.

Тут особлива увага повинна приділятися гарантії, що підготовлений огляд – повний. Пропуск тільки одного критичного підключення може підірвати всю систему безпеки. Тому, наприклад, усі модеми, що використовуються, повинні бути зареєстровані, тому що потенційно критичні підключення до зовнішнього світу можуть бути здійснені з них.

Виконання:

– Реєстрація зовнішніх з'єднань;

– Визначення підключень, які використовуються для передачі важливої інформації;

– Визначення ліній зв'язку, які не повинні використовуватися для передачі критично важливої інформації;

– Реєстрація всіх критичних ліній зв'язку в табличному або графічному вигляді.

Таблиця 2.7. Основні критичні з'єднання

	Чому критично				
З'єднання	**K1 зовнішнє підключення**	**K2 Висока конфіденційність**	**K3 Висока цілісність**	**K4 Висока доступність**	**K5 Не передається**
N1 - Інтернет	X				
N5 - N6	X				
S1 - N4		X			
S3 - N3				X	
S4 - N3				X	
S5 - N3				X	
C1 - N4		X			
N1 - N2				X	X
N2 - N3				X	
N4 - N3					X

сної допомоги неавторизованому користувачеві. Належна процедура входу повинна:

а) не відображати ідентифікатори системи або застосунку до тих пір, поки процес входу не завершений успішно;

б) виводити загальне попередження, що доступ до комп'ютера надається тільки авторизованим користувачам;

в) не давати підказок під час процедури входу, які могли б допомогти неавторизованому користувачу;

г) здійснювати підтвердження інформації для входу тільки після завершення введення даних. При виявленні помилки система не повинна вказувати, яка частина даних вірна або невірна;

д) захищати від спроб входу методом повного перебору (або «грубої сили» – brute force);

е) реєструвати неуспішні і успішні спроби;

ж) фіксувати інцидент безпеки при виявленні спроб або факту успішного порушення процедур входу;

з) відображати наступну інформацію після успішного завершення процедури входу:

1) дата і час попереднього успішного входу;

2) деталі усіх невдалих спроб входу з моменту останнього успішного входу;

и) не відображати пароль, що вводиться;

к) не передавати пароль відкритим текстом по мережі;

л) завершувати неактивну сесію після певного періоду простою, особливо якщо є високий ризик, пов'язаний з місцезнаходженням, наприклад, в громадському місці або за межами дії СМІБ організації, або роботою з мобільного пристрою;

м) обмежувати час з'єднання для забезпечення додаткового захисту застосунків з високим ризиком і зниження можливості несанкціонованого доступу.

Паролі є широко застосовуваним способом забезпечення ідентифікації та авторизації, заснований на використанні інформації, яку знає тільки користувач. Той же результат може бути отриманий при використанні криптографічних методів і протоколів авторизації. Строгість процедури авторизації користувача повинна відповідати категорії інформації, до якої здійснюється доступ.

Застосування пароля:

– локальна система;

жуть також посилювати наслідки розкриття таємної інформації автентифікації.

Контроль доступу до систем та прикладних програм.

Ціль: Запобігти несанкціонованому доступу до систем та прикладних програм.

1) Обмеження доступу до інформації. Доступ до інформації та функцій прикладних систем має бути обмежений відповідно до визначеної політики контролю доступу.

Обмеження доступу повинні ґрунтуватися на вимогах конкретних бізнес-додатків і відповідати встановленій політиці контролю доступу.

Для забезпечення виконання вимог щодо обмеження доступу має бути прийнято до уваги наступне:

а) надання меню для управління доступом до функцій системного застосування;

б) перевірка, до яких даних може мати доступ конкретний користувач;

в) перевірка прав доступу користувача, наприклад, на читання, видалення або виконання;

г) перевірка прав доступу до інших додатків;

д) обмеження на інформацію, що міститься в результатах роботи програми;

е) забезпечення фізичних і логічних засобів контролю доступу для ізолювання уразливих додатків, даних або систем.

2) Процедури безпечного підключення (log-on). Доступ до систем та прикладних програм повинен контролювати процедурою безпечного підключення, коли це визначено політикою контролю доступу.

Повинні бути вибрані відповідні методи автентифікації для підтвердження введеної ідентифікаційної інформації користувача.

Там, де потрібна строга перевірка автентифікаційної і ідентифікаційної інформації, повинні бути використані додаткові заходи автентифікації, такі як криптографічні засоби, смарт-карти, апаратні ключі або біометричні засоби.

Процедури для входу в систему або застосунку повинні бути розроблені так, щоб мінімізувати можливість несанкціонованого доступу. Тобто процедури входу повинні надавати мінімум інформації про систему або застосунок, щоб уникнути надання ненавми-

Визначення вимоги безпеки для ділянок

Вимоги безпеки до відповідних будівель і ділянок виходять із результатів визначення вимог безпеки для IT-систем. Ці вимоги безпеки виходять з вимог безпеки для IT-систем, встановлених на відповідних ділянках, інформації, яку обробляють, або носіїв даних, які там зберігаються – використовуючи принцип максимуму. Під час оцінки слід розглянути можливість сукупного ефекту, де на одній ділянці розташовано відносно велика кількість IT-систем, як, наприклад, часто буває в серверних кімнатах. До того ж, обґрунтування оцінених вимог безпеки слід задокументувати. Запис необхідної інформації в таблицю (див. табл. 2.8) є також корисним для цього і ґрунтується на огляді ділянок, що був виконаний раніше.

Приклад:

Bundesamt für Organisation und Verwaltung (Федеральна служба організації та адміністрування, Federal Agency for Organisation and Administration, BOV). Таблиця 2.8, наведена нижче, показує отримані для BOV результати:

Таблиця 2.8. Вимоги безпеки до відповідних будівель і ділянок

Ділянка			IT / Інформація	Вимоги безпеки		
Ім'я	**Тип**	**Розміщення**	**IT-системи / Носії даних**	**Конфіденційність**	**Цілісність**	**Доступність**
1	2	3	4	5	6	7
R U.02	Архів носіїв даних	Будівля в Бонні	Резервування носіїв (щотижневе резервування серверів від S1 до S5)	Високі	Високі	Нормальні
R B.02	Технологічна ділянка	Будівля в Бонні	Телекомунікаційні системи	Нормальні	Нормальні	Високі
R 1.01	Серверна кімната	Будівля в Бонні	S1, N4	Високі	Високі	Нормальні
R 1.02 - R 1.06	Офіси	Будівля в Бонні	C1	Високі	Нормальні	Нормальні

Закінчення табл. 2.8

1	2	3	4	5	6	7
R 3.11	Захисна шафа на ділянці R 3.11	Будівля в Бонні	Резервування носіїв (щотижневе резервування серверів від S1 до S5)	Високі	Високі	Нормальні
R E.03	Серверна кімната	Будівля в Берліні	S6, N6, N7	Нормальні	Високі	Високі
R 2.01 - R 2.40	Офіси	Будівля в Берліні	C4, деякі з факсами	Нормальні	Нормальні	Нормальні

Виконання:

– Отримати вимоги безпеки для ділянок із вимог безпеки IT-систем і додатків;

– Розглянути залежності, принцип максимуму і, якщо буде необхідність, сукупний ефект або ефект поширення;

– Записати результати й чіткі обґрунтування.

Обробка результатів визначення вимог безпеки

Результати, отримані після визначення вимог безпеки, є відправною точкою, від якої починають розробляти концепцію безпеки IT. Для захисту, який виходить за межі стандартних заходів безпеки, рекомендованих IT-Grundschutz, прийняті такі пункти для категорій вимог безпеки (див. табл. 2.9):

Таблиця 2.9. Категорії вимог безпеки

Захисний ефект стандартних заходів безпеки IT-Grundschutz	
Вимоги безпеки категорії «нормальні»	Заходи безпеки стандарту IT-Grundschutz в основному відповідні і обґрунтовані
Вимоги безпеки категорії «високі»	Заходи безпеки стандарту IT-Grundschutz надають основний рівень захисту, але їх недостатньо. Додаткові заходи безпеки можуть бути визначені після виконання додаткового аналізу безпеки.
Вимоги безпеки категорії «дуже високі»	Заходи безпеки стандарту IT-Grundschutz надають основний рівень захисту, але в загальному їх недостатньо. Необхідні додаткові заходи безпеки повинні визначатися індивідуально на основі додаткового аналізу.

2) не використовують такого, про що будь-хто може легко здогадатися або обчислити на основі особистої інформації, наприклад, імен, номерів телефонів, дат народження та ін.;

3) невразливі для словникової атаки (тобто не складається зі слів, включених в словники);

4) не містить послідовності однакових цифр або символів;

5) будучи тимчасовими, змінюються у першу сесію підключення;

д) не ділитися таємною інформацією автентифікації;

е) забезпечувати належний захист паролів в тих випадках, коли паролі використовуються в якості таємної інформації автентифікації в автоматизованих процедурах входу і зберігаються в системі;

ж) не використовувати один і той же пароль для ділових і приватних цілей.

Таблиця 4.3. Приклад критеріїв для паролів

Хороший пароль	**Поганий пароль**
1) довгий (8-12-15 символів); 2) містить як великі, так і малі латинські літери; 3) містить цифри; 4) не знайдеться в словнику, це не ім'я і не українське слово (ckjdj), набране у латинській розкладці; 5) ніяк не пов'язаний з власником; 6) змінюється періодично або за потреби; 7) не є улюбленим – різні паролі для різних входів; 8) його можливо запам'ятати.	1) короткий (менше 8 символів); 2) все в одному регістрі (всі ВЕЛИКІ погано як і всі маленькі); 3) не містить цифр; 4) знайдеться в словнику, це ім'я або українське слово (ckjdj), набране у латинській розкладці; 5) будь-яким чином пов'язаний з власником; 6) не змінюється роками ні за яких обставин; 7) може бути улюбленим – один пароль усюди; 8) його неможливо забути.

Застосування технології єдиного входу в систему (SSO) або інших засобів управління таємною інформацією автентифікації знижує обсяг таємної інформації автентифікації, яку вимагають від користувача для захисту, і, таким чином, може збільшувати результативність даного методу реалізації. Однак, такі інструменти мо-

б) поточні обов'язки співробітника, зовнішнього користувача чи іншого користувача;

в) цінність активів, які перебувають в поточному доступі.

У певних обставинах права доступу можуть бути призначені більш широкому колу людей, ніж співробітники, які звільняються або зовнішні користувачі, наприклад, ідентифікаційні дані групи. В такому випадку співробітники, які звільняються повинні бути виключені з будь-якого списку групових прав доступу та повинні бути вжиті заходи, щоб повідомити всіх інших співробітників і зовнішніх користувачів про те, щоб не передавати більш цю інформацію такому співробітнику.

У тому випадку, коли припинення відносин ініційовано керівництвом, незадоволені співробітники або зовнішні користувачі можуть навмисно пошкодити інформацію або перешкоджати роботі засобів обробки інформації. Співробітники, які звільнилися або звільнені можуть спробувати скопіювати інформацію для майбутнього використання.

Відповідальності користувача.

Ціль: Зробити користувачів відповідальними за збереження їх інформації автентифікації.

Використання таємної інформації автентифікації. Треба вимагати від користувачів додержання визначених в організації практик у використанні таємної інформації автентифікації.

Всім користувачам повинно бути рекомендовано:

а) зберігати конфіденційність таємної інформації автентифікації, гарантуючи, що вона не буде розголошена іншій стороні, включаючи представників органів влади;

б) уникати записувати (наприклад, на листку паперу, в файлах або мобільних пристроях) таємну інформацію автентифікації, крім тих випадків, коли ці записи можуть бути надійно збережені і використовується схвалений спосіб запису (наприклад, програма Password Vault);

в) змінити таємну інформацію автентифікації в тому випадку, коли є які-небудь ознаки її можливої компрометації;

г) в тих випадках, коли в якості таємної інформації автентифікації використовуються паролі, задавати стійкі паролі з достатньою мінімальною довжиною, які (див. табл. 4.3):

1) легко запам'ятовуються;

Якщо вимоги безпеки для IT-системи визначені як «нормальні», досить усюди впровадити заходи безпеки стандарту IT-Grundschutz. Додатковий аналіз безпеки повинен бути запланований для IT-систем, мережевих з'єднань і ділянок використання IT, які мають «високі» або іноді навіть «дуже високі» вимоги безпеки. До того ж, високі вимоги безпеки повинні братися до уваги для цих елементів при обробці «додаткових» заходів безпеки. Тому, наприклад, заходи безпеки S 1.10 *Використання захисних дверей* можуть бути необов'язковими на серверній ділянці, на якій нормальні вимоги безпеки, а там, де потрібен високий рівень конфіденційності, можуть бути обов'язковою умовою.

Області зі змінними вимогами безпеки

При визначенні вимог безпеки часто виявляється, що серед розглянутих ресурсів IT є області, в яких обробляється інформація з високими або дуже високими вимогами захисту. Більш високі вимоги безпеки в одній області передаються в іншу за принципом максимуму. Навіть якщо тільки кілька елементів даних мають більш високі вимоги безпеки, сильний зв'язок і взаємодія IT-систем і додатків швидко призводить до більш високих вимог безпеки, переданих в інші області, використовуючи принцип максимуму.

Отже, повинні встановлюватися зони безпеки, щоб обмежити ризики і витрати. Такі зони безпеки можуть характеризуватися в термінах ділянок, технологій або персоналу.

Приклади:

– Географічні зони безпеки: немає необхідності постійно блокувати або спостерігати окремо кожен офіс, зони з великою кількістю відвідувачів слід відокремити від областей, які мають високі вимоги безпеки. Тому, ділянки зустрічей, навчання і подій, а також буфет, які залучають зовнішніх клієнтів, слід розмістити недалеко від входу в будівлю. Тоді для співробітника безпеки можливо контролювати доступ у частину будівлі з офісами на вході. Особливо важливі області, такі як відділ розробки, повинні мати додатковий контроль доступу, наприклад, чіпові карти.

– Технічні зони безпеки: щоб обмежити доступ до конфіденційних даних у певних областях у межах мережі й щоб запобігти впливу помилок або атак на окремі елементи або на функції, корисно розділити мережу на декілька підмереж.

– Зони безпеки персоналу: кожна особа повинна бути наділена тільки тими правами, які необхідні їй для виконання завдань, що доручені керівництвом. До того ж, існують різні ролі, які одна особа ніколи не повинна виконувати одночасно. Наприклад, аудитор не повинен працювати в бухгалтерії або адміністрації IT одночасно, тому що він не може перевіряти сам себе. Щоб спростити призначення прав доступу, люди, що виконують функції, які не можуть поєднуватися, повинні працювати в різних групах або відділах.

Якщо області зі схожими вимогами безпеки відповідно перебудовані вже на етапі планування, це скорочує багато роботи на всіх етапах, аж до перевірки.

Виконання:

– Перевірити, чи можна об'єкти з підвищеними вимогами безпеки зібрати в зонах безпеки;

– Визначити об'єкти з підвищеними вимогами безпеки для додаткового аналізу їх захисту [4].

Робота СМІБ за вимогами ISO 27001 (рис. 2.12)

Контекст організації

Розуміння організації і її контексту

Організація повинна визначати зовнішні та внутрішні проблеми, що мають відношення до її мети та впливають на здатність досягти передбачуваного результату в системі управління ІБ.

Рис. 2.12. Структура стандарту

Розуміння потреб та очікувань зацікавлених сторін

Організація повинна визначити:

а) права доступу користувачів слід переглядати через певні інтервали часу, так і після змін, таких як підвищення або пониження на посаді, або припинення трудових відносин;

б) права доступу користувача повинні переглядатися і перепризначатися у разі зміни його ролі в організації;

в) привілейовані права доступу повинні переглядатися частіше;

г) призначені привілеї повинні перевірятися через регулярні проміжки часу, щоб гарантувати, що ніхто не отримав привілеї несанкціонованим чином;

д) зміни в привілейованих акаунтах повинні реєструватися для періодичного перегляду.

6) Вилучення або корекція прав доступу. Права доступу всього найманого персоналу та користувачів зовнішніх сторін до інформації та засобів оброблення інформації мають вилучатися після припинення найму, контракту чи угоди, або коректуватися після змін.

Після завершення трудових відносин права доступу користувача до інформації та активів, пов'язаних із пристроями обробки інформації і службами, повинні бути скасовані або припинені. Зміни на посаді повинні знаходити відображення в скасуванні всіх прав доступу, що не були схвалені для нової позиції. Права доступу, які повинні бути скасовані або скориговані, поширюються також на фізичний і логічний доступ. Скасування або коригування можуть бути виконані за допомогою видалення, скасування або заміни ключів, ідентифікаційних карт, пристроїв обробки інформації або абонементів. Будь-яка документація, яка вказує на права доступу співробітника або працюючого за контрактом, повинна відображати скасування або коригування прав доступу. Якщо співробітник, який звільняється або зовнішній користувач знає паролі для логінів активних користувачів, ці паролі повинні бути змінені після завершення або зміни працевлаштування, контракту або угоди.

Права доступу до інформації та активів, пов'язаних із пристроями обробки інформації, повинні бути знижені або скасовані до припинення трудових відносин або їх зміни, в залежності від оцінки ризику, пов'язаного з такими факторами, як:

а) чи були зміни або припинення трудових відносин ініційовані працівником, зовнішнім користувачем або керівництвом, а також причини припинення відносин;

користувачів потрібно контролювати за допомогою офіційно оформленого процесу управління.

Цей процес повинен включати в себе наступні вимоги:

а) користувачі повинні підписати угоду, за якою зобов'язалися зберігати конфіденційність особистої секретної інформації автентифікації і зберігати групову (тобто використовувану кількома користувачами) таємну інформацію автентифікації виключно в межах групи (така підписана угода може бути частиною трудової угоди);

б) у тих випадках, коли користувачі повинні самі забезпечувати збереження своєї таємної інформації для автентифікації, їм на початку повинна бути видана тимчасова таємна інформація автентифікації, яку вони повинні змінити при першому сеансі;

в) повинні бути встановлені процедури перевірки ідентичності користувача перед видачею нової або заміною таємної інформації автентифікації, а також при видачі тимчасової таємної інформації автентифікації;

г) тимчасова таємна інформація автентифікації слід передати користувачеві безпечним способом, слід уникати використання зовнішніх сторін або незахищених (відкритим текстом) повідомлень електронної пошти;

д) тимчасова таємна інформація автентифікації повинна бути унікальною для конкретного користувача і не повинна бути легко вгадуваною;

е) користувачі повинні підтвердити отримання таємної інформації автентифікації;

ж) таємна інформація автентифікації, встановлена за замовчуванням виробником, повинна бути змінена після установки системи або ПЗ.

Паролі є різновидом таємної інформації автентифікації, який широко застосовується, а також – типовим засобом перевірки автентичності користувача. Іншим видом таємної інформації автентифікації є криптографічні ключі, а також інші дані, що зберігаються на апаратних ключах (наприклад, смарт-картках), які генерують коди для автентифікації.

5) Перегляд прав доступу користувача. Власники активів СМІБ повинні переглядати права доступу користувача через регулярні встановлені інтервали.

При перегляді прав доступу має враховуватися наступне:

а) зацікавлені сторони, які мають відношення до системи управління інформаційною безпекою;

б) вимоги цих зацікавлених сторін щодо інформаційної безпеки.

Визначення сфери застосування системи управління ІБ

Організація повинна визначити межі та можливість застосування СМІБ для встановлення її сфери застосування.

Для визначення сфери застосування організація повинна розглянути:

а) зовнішні та внутрішні обставини;

б) вимоги; та

в) інтерфейси та залежності між діями, які виконує організація, і тими, що виконують інші організації.

Сфера застосування має бути доступною як документована інформація.

Система управління інформаційною безпекою

Організація повинна розробити, впровадити, підтримувати та постійно вдосконалювати систему ІБ відповідно до вимог стандарту [1-3].

2.6. Забезпечення СМІБ

Ресурси

Організація повинна визначити й забезпечувати наявність ресурсів, потрібних для розроблення, впровадження, підтримання й постійного вдосконалення СМІБ.

Компетенція

Організація повинна:

а) визначити рівень необхідної компетентності персоналу, який виконує роботи, що впливають на результативність ІБ;

б) гарантувати, що цей персонал має компетенцію на основі відповідного навчання, тренінгів або досвіду;

в) за можливості, забезпечувати виконання певних дій для досягнення необхідної компетенції та оцінювати ефективність таких дій;

г) зберігати відповідну документовану інформацію як доказ компетентності.

Обізнаність

Персонал, який виконує функції під наглядом організації, повинен бути обізнаним в:

а) політиці ІБ;

б) його вкладі в ефективність СМІБ, враховуючи переваги від вдосконалення результативності ІБ;

в) розумінні невідповідності вимогам СМІБ.

Комунікація

Організація повинна визначити потребу у внутрішніх та зовнішніх комунікаціях з питань СМІБ, включаючи:

а) з яких питань спілкуватися;

б) коли спілкуватися;

в) з ким спілкуватися;

г) хто повинен спілкуватися;

д) процеси, за допомогою яких комунікація повинна відбуватися.

Документована інформація

Загальні положення

Система СМІБ організації повинна включати:

а) документовану інформацію, визначену цим стандартом;

б) документовану інформацію, визначену організацією як необхідну для ефективності СМІБ.

Створення та оновлення

У разі створення й оновлення документованої інформації організація повинна гарантувати відповідну:

а) ідентифікацію та опис (наприклад, назву, дату, автора чи посилальний номер);

б) формат (наприклад, мову, версію програмного забезпечення, графіки) та носії (наприклад, папір, електронні);

в) перегляд і затвердження для відповідності й адекватності.

Контроль документованої інформації

Задокументована інформація, визначена СМІБ та цим стандартом має контролювати для гарантії того, що:

а) вона доступна й придатна для використання, де і коли вона потрібна;

б) її належним чином захищено (наприклад, від втрати конфіденційності, помилкового використання або втрати цілісності).

Для контролю документованої інформації організація повинна виконувати такі дії відповідним чином:

а) розподіл, доступ, повернення та використання;

а) привілейовані права доступу, пов'язані з кожною системою або процесом, наприклад, ОС, СУБД і кожним додатком, а також користувачами, яким потрібно призначення таких прав, повинні бути визначені;

б) привілейовані права доступу повинні бути призначені користувачам за принципом «доступ за потребою» і «доступ за подією» відповідно до політики контролю доступу, тобто по мінімуму, виходячи з їх функціональних завдань;

в) процес авторизації і реєстрація всіх призначених привілеїв повинні підтримуватися у керованому стані. Привілейовані права доступу не повинні присвоюватися до завершення процесу авторизації;

г) повинні бути визначені вимоги для встановлення терміну дії привілейованих прав доступу;

д) привілейовані права доступу повинні бути пов'язані з ідентифікатором користувача, відмінним від того, що використовується для виконання повсякденних посадових обов'язків. Ці обов'язки не повинні виконуватися під привілейованим ідентифікатором;

е) повноваження користувачів з привілейованими правами доступу повинні регулярно переглядатися з метою того щоб переконатися, що вони відповідають їх обов'язкам;

ж) повинні бути розроблені і підтримуватися конкретні процедури для уникнення неавторизованого використання загальних адміністраторських ідентифікаторів відповідно до можливостей конфігурації системи;

з) для стандартних адміністраторських ідентифікаторів при колективному їх використанні повинна забезпечуватися конфіденційність секретної інформації для автентифікації (наприклад, часта зміна паролів, а також максимально їх швидка зміна при звільнені користувача з привілейованими правами або зміні його обов'язків, передача їх всім користувачам з привілейованими правами за допомогою відповідних механізмів).

Невідповідне використання привілеїв, пов'язаних з адмініструванням системи (будь-якої функції або ІС, яка дозволяє користувачеві змінити засоби управління системою або додатком) є основним фактором збоїв і порушення функціонування системи.

4) Управління таємною інформацією автентифікації користувачів. Облік таємної інформації автентифікації

– призначення або скасування прав доступу для цього ідентифікатора користувача.

2) Забезпечення доступу користувачів. Має бути впроваджено формально затверджений процес забезпечення доступу користувачу для надання або вилучення прав доступу для всіх типів користувачів до всіх систем та послуг.

Процес, що забезпечує призначення або скасування прав, пов'язаних з ідентифікаторами користувача, повинен включати:

а) отримання дозволу від власника інформаційної системи або служби на використання цієї ІС або служби, так само може бути доцільним відділення підтвердження прав доступу від управління;

б) перевірку того, що надається рівень доступу відповідає політикам доступу й узгоджується з іншими вимогами, такими, як поділ обов'язків;

в) гарантію того, що права доступу не будуть активовані (наприклад, постачальниками послуг) до завершення процедур авторизації;

г) ведення централізованої реєстрації прав доступу, що пов'язуються з ідентифікатором користувача, до ІС і службам;

д) зміна прав доступу користувачам, у яких помінялися ролі або завдання, а також негайне скасування або блокування прав доступу користувачам, що пішли з організації;

е) періодичний перегляд прав доступу з власниками ІС і служб.

Слід розглянути питання про введення визначаючих правил доступу ролей, що випливають з вимог бізнесу, які об'єднують різні права доступу в типові профілі доступу користувачів. Запити на доступ і їх аналіз легше обробляються на рівні таких ролей, ніж на рівні окремих прав.

Слід розглянути питання включення в контракт співробітника і контракт на надання послуг розділів, що визначають санкції в разі спроби несанкціонованого доступу, який здійснюють співробітники або працюючи за контрактом

3) Управління привілейованими правами доступу. Призначення та використання привілейованих прав доступу має бути обмежено та контрольовано.

Розподіл привілейованих прав доступу має контролюватися через формалізований процес авторизації відповідно до діючої політики контролю доступу. Повинні бути передбачені наступні кроки:

б) збереження та консервування, зокрема й консервування чіткості/розбірливості;

в) контроль змін (наприклад, контроль версій);

г) утримування й розташування.

Документована інформація від зовнішнього джерела, визначена організацією як необхідна для планування та функціонування СМІБ, має бути ідентифікована відповідних чином і контрольована [1, 2].

Системний підхід до опису ІБ пропонує виділити такі складові ІБ

1) Законодавча, нормативно-правова та наукова база.

2) Структура і завдання органів (підрозділів), що забезпечують безпеку ІТ.

3) Організаційно-технічні і режимні заходи і методи (Політика ІБ).

4) Програмно-технічні засоби і способи забезпечення ІБ.

Метою реалізації ІБ будь-якого об'єкта є побудова системи забезпечення ІБ даного об'єкту. Для побудови та ефективної експлуатації системи забезпечення ІБ необхідно:

– виявити вимоги ЗІ, специфічні для даного об'єкта захисту;

– врахувати вимоги національного та міжнародного Законодавства;

– використовувати напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення ІБ;

– визначити підрозділи, відповідальні за реалізацію та підтримку системи забезпечення ІБ;

– розподілити між підрозділами області відповідальності у здійсненні вимог системи забезпечення ІБ;

– на базі управління ризиками ІБ визначити загальні положення, технічні та організаційні вимоги, що становлять Політику ІБ об'єкта захисту;

– реалізувати вимоги Політики ІБ, впровадивши відповідні програмно-технічні засоби і способи ЗІ;

– реалізувати СМІБ;

– використовуючи СМІБ організувати регулярний контроль ефективності системи забезпечення ІБ і при необхідності перегляд та коригування системи забезпечення ІБ і СМІБ.

Як видно з останнього етапу робіт, процес реалізації системи забезпечення ІБ безперервний і циклічно (після кожного перегляду) повертається до першого етапу, повторюючи послідовно всі інші. Так системи забезпечення ІБ коригується для ефективного виконання своїх завдань ЗІ та відповідності новим вимогам ІС, яка постійно оновлюється.

1. Організаційно-технічні і режимні заходи і методи.

Для опису технології ЗІ конкретної ІС зазвичай будується так звана Політика ІБ або Політика безпеки розглянутої ІС.

Політика безпеки (інформації в організації) (англ. Organizational security policy) – сукупність документованих правил, процедур, практичних прийомів або керівних принципів у галузі безпеки інформації, якими керується організація у своїй діяльності.

Для побудови Політики ІБ рекомендується окремо розглядати такі напрями захисту ІС:

– захист об'єктів ІС;

– захист процесів, процедур і програм обробки інформації;

– захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні, радіоканали та ін.);

– придушення побічних електромагнітних випромінювань і наведень;

– управління системою захисту.

При цьому по кожному з перерахованих вище напрямків Політика ІБ повинна описувати наступні етапи створення засобів ЗІ:

1) визначення інформаційних і технічних ресурсів, що підлягають захисту;

2) виявлення повної множини потенційно можливих загроз і каналів витоку інформації;

3) проведення оцінки уразливості й ризиків інформації за наявної множини загроз і каналів витоку;

4) визначення вимог до системи захисту;

5) здійснення вибору засобів ЗІ та їх характеристик;

6) впровадження та організація використання обраних заходів, способів та засобів захисту;

7) здійснення контролю цілісності й керування системою захисту.

д) вимоги до авторизації користувача для доступу до різних мережевих служб;

е) моніторинг використання мережевих служб.

Політика використання мережевих служб повинна бути узгодженою з політикою контролю доступу організації.

Несанкціоноване або незахищене підключення до мережевих служб може впливати на всю організацію. Контроль цього особливо важливий для мережевих з'єднань додатків, критично важливих з точки зору бізнесу, або для користувачів, що знаходяться в місцях із високим рівнем ризику, наприклад, громадських місцях або точках за межами організації, які поза контролем СМІБ організації.

Управління доступом користувача.

Ціль: Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.

1) Реєстрація та зняття з реєстрації користувача. Має бути впроваджено процес реєстрації та зняття з реєстрації для того, щоб була можливість управляти правами доступу.

Процес управління ідентифікаторами користувачів повинен включати в себе:

а) використання унікального ідентифікатора користувача, що дозволяє зв'язати користувачів з їхніми діями і нести за них відповідальність;

б) використання колективних ідентифікаторів має бути дозволено тільки в тих випадках, коли це необхідно для бізнесу або в силу операційних причин і має бути затверджене та задокументовано;

в) негайне блокування або видалення ідентифікатора користувача, якщо він покинув організацію;

г) періодичне виявлення й видалення або блокування неактуальних ідентифікаторів;

д) гарантію того, що неактуальні ідентифікатори не видаються іншим користувачам.

Забезпечення або скасування доступу до інформації або пристроїв обробки інформації зазвичай є двокроковою процедурою:

– призначення та активація або скасування ідентифікатора користувача;

а) встановлення правил, за наступним принципом «Заборонено все, що не дозволено», ніж «Дозволено все, що не заборонено»;

б) зміни маркування інформації, які ініціюються автоматично пристроями обробки інформації і які ініційовані рішенням користувача;

в) зміни в повноваженнях користувача, які ініціюються автоматично ІС і які ініційовані адміністратором;

г) правила, які вимагають певної процедури затвердження до вступу в силу, і ті, які цього не вимагають;

16) Правила контролю доступу повинні бути зафіксовані в формальних процедурах і під них визначені обов'язки.

17) Контроль доступу на основі ролей є підходом, який успішно використовується багатьма організаціями для зв'язку прав доступу й бізнес-ролей.

18) Є два принципи, що визначають політику контролю доступу і які часто застосовуються:

– «знає той, кому належить знати»: ви отримуєте доступ тільки до тієї інформації, яка необхідна для виконання службових завдань (різні завдання/ролі мають на увазі різну необхідність і, отже, різний профіль доступу);

– «доступ за потребою»: ви отримуєте доступ тільки до тих пристроїв обробки інформації (IT-обладнання, додатки, процедури, приміщення), які необхідні вам для виконання завдання/роботи/ролі.

2) Доступ до мереж та послуг мережі. Користувачі повинні отримувати доступ до мережі та послуг мережі лише тоді, коли вони були спеціально авторизовані для використання.

Повинна бути сформульована політика, яка відноситься до використання мереж і мережевих служб. Ця політика повинна охоплювати:

а) мережі й мережеві служби, до яких дозволений доступ;

б) процедури авторизації для визначення, кому до якої мережі або службі дозволений доступ;

в) засоби управління і процедури для захисту доступу до мережевих з’єднань і мережевих служб;

г) засоби для доступу до мереж і мережевих служб (наприклад, використання VPN або бездротової мережі);

Політика ІБ оформляється у вигляді задокументованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями опису (деталізації) процесу захисту.

Документи верхнього рівня Політики ІБ відображають позицію організації до діяльності в галузі ЗІ, її прагнення відповідати державним, міжнародним вимогам і стандартам у цій галузі. Подібні документи можуть називатися «Концепція ІБ», «Регламент управління ІБ», «Політика ІБ», «Технічний стандарт ІБ» і т. ін. Сфера поширення документів верхнього рівня зазвичай не обмежується, проте дані документи можуть випускатися і в двох редакціях – для зовнішнього і внутрішнього використання.

До середнього рівня відносять документи, що стосуються окремих аспектів ІБ. Це вимоги на створення та експлуатацію засобів ЗІ, організацію інформаційних та бізнес-процесів організації по конкретному напрямку ЗІ. Наприклад: Безпеки даних, Безпеки комунікацій, Використання засобів криптографічного захисту, Контентна фільтрація тощо. Подібні документи зазвичай видаються у вигляді внутрішніх технічних і організаційних політик (стандартів) організації. Усі документи середнього рівня політики ІБ конфіденційні.

У політику ІБ нижнього рівня входять регламенти робіт, керівництва з адміністрування, інструкції з експлуатації окремих сервісів ІБ.

2. Організаційний захист об'єктів ІС.

Організаційний захист – це регламентація виробничої діяльності й взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз. Організаційний захист забезпечує:

– організацію охорони, режиму, роботу з кадрами, з документами;

– використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх і зовнішніх загроз підприємницької діяльності.

До основних організаційних заходів належать:

– організація режиму й охорони. Їх мета – виключення можливості таємного проникнення на територію й у приміщення сторонніх осіб;

– організація роботи зі співробітниками, яка передбачає добір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил ЗІ та ін.;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки й використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;

– організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;

– організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах.

3. Програмно-технічні засоби і способи забезпечення ІБ.

Класифікація засобів захисту інформації.

– Засоби захисту від несанкціонованого доступу (НСД):
  - ✓ засоби авторизації;
  - ✓ мандатне управління доступом;
  - ✓ виборче управління доступом;
  - ✓ управління доступом на основі ролей;
  - ✓ журналювання (так само називається Аудит).

– Системи аналізу та моделювання інформаційних потоків (CASE-системи).

– Системи моніторингу мереж:
  - ✓ системи виявлення й запобігання вторгнень (IDS / IPS).
  - ✓ системи запобігання витоків конфіденційної інформації (DLP-системи).

4.5. Управління доступу

Бізнес-вимоги до контролю доступу.

Ціль: Обмежити доступ до інформації та засобів оброблення інформації.

1) Політика контролю доступу. Політика контролю доступу має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та ІБ.

Власники активів повинні визначити відповідні правила для контролю доступу, права доступу й обмеження для певних категорій користувачів щодо їхніх активів із рівнем деталізації і строгості контролю, що відображає ризики, пов'язані з ІБ.

Засоби контролю доступу можуть бути як логічними, так і фізичними і вони повинні розглядатися спільно. Користувачам і постачальникам сервісів повинні бути чітко і зрозуміло доведені вимоги бізнесу, яким повинні задовольняти засоби контролю доступу.

Політика контролю доступом повинна враховувати наступне:

а) вимоги щодо безпеки бізнес-додатків;

б) політики поширення і авторизації інформації, наприклад, принцип «знає той, кому належить знати», рівні ІБ і класифікації інформації;

в) відповідність між правами доступу й політиками класифікації інформації для систем і мереж;

г) відповідні законодавчі та будь-які контрактні зобов'язання, що стосуються обмеження доступу до даних або сервісів;

д) управління правами доступу в розподілених середовищах і мережах, які допускають усі типи з'єднань;

е) поділ завдань по контролю доступу, наприклад, запит доступу, авторизація доступу, адміністрування доступу;

ж) вимоги до авторизації запитів на доступ;

з) вимоги до періодичного перегляду прав доступу;

и) скасування прав доступу;

к) архівування записів всіх значущих подій, що стосуються використання та управління ідентифікаційною інформацією користувачів і таємною інформацією для автентифікації;

л) завдання з привілейованим доступом.

Слід проявляти обережність при формулюванні правил контролю доступу, з огляду на:

– інтеграція з іншими системами;
– платформа розробки.

Для реалізації системи була використана сучасна платформа розробки XAFARI (на основі технологічної платформи компанії Developer Express). Її широкі можливості дозволяють не тільки зробити гнучку настройку під потреби замовника, інтегрувати «Галактика ЕАМ» з вже використовуваними на підприємстві додатками, але і здійснити дані роботи з мінімальними тимчасовими й фінансовими витратами.

XAFARI – багатофункціональна модульна платформа для побудови розподілених систем управління підприємством в сервіс–орієнтованої Web-архітектурі (SOBA Service-Oriented Business Application). В якості технології розробки використовується програмна платформа Microsoft.NET Framework з використанням мови C # [11].

Переваги платформи розробки XAFARI [11]:
– сучасна і зручна ергономіка;
– одна з найпоширеніших у світі платформ;
– світова спільнота розробників XAF;
– багато готових компонент і візуальних об'єктів;
– швидкий розвиток і якісна підтримка платформи;
– візуальна частина розробляється без програмування;
– редактор моделі дозволяє налаштувати багато елементів;
– спадкування властивостей об'єктів системи;
– сучасна платформа розробки XAFARI забезпечує:
  ✓ зручний і наочний інтерфейс користувача;
  ✓ високий рівень кастомізації під потреби замовника;
  ✓ спрощена схема інтеграції зі сторонніми рішеннями;
  ✓ сучасна платформа розробки;
  ✓ можливість використання кожного СУБД;
  ✓ відкритість коду і наявність великого числа сертифікованих фахівців;
  ✓ підтримка безлічі СУБД;
  ✓ Win- і Web-клієнти;
  ✓ мобільний клієнт.

– Аналізатори протоколів.
– Антивірусні засоби.
– Міжмережеві екрани.
– Криптографічні засоби:
  ✓ шифрування;
  ✓ цифровий підпис.
– Системи резервування:
  ✓ резервне копіювання;
  ✓ відмовостійкий кластер;
  ✓ резервний центр обробки даних (ЦОД) для катастрофостійкої ІС.
– Системи безперебійного живлення:
  ✓ джерела безперебійного живлення;
  ✓ резервні лінії електроживлення;
  ✓ генератори електроживлення.
– Системи автентифікації на основі:
  ✓ пароля;
  ✓ ключа доступу (фізичного або електронного);
  ✓ сертифікату;
  ✓ біометричних даних.
– Засоби запобігання злому корпусів і крадіжок устаткування.
– Засоби контролю та управління доступом в приміщення.
– Інструментальні засоби аналізу систем захисту.
– Засоби захисту від побічних електромагнітних випромінювань та наведень [5].

2.7. Функціонування СМІБ

Робоче планування й контроль

Організація повинна планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог ІБ, а також впроваджувати дій щодо ризиків та можливостей. Організація також повинна впроваджувати плани для досягнення цілей ІБ.

Організація повинна зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано.

Організація повинна контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби.

Організація повинна гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані.

Оцінювання ризиків ІБ

Організація повинна виконувати оцінювання ризиків через заплановані або запропоновані інтервали, чи коли відбуваються суттєві зміни з урахуванням критеріїв:

1) критерії прийняття ризиків;

2) критерії для виконання оцінки ризиків ІБ.

Організація повинна зберігати задокументовану інформацію стосовно результатів оцінювання ризиків ІБ.

Оброблення ризиків ІБ

Організація повинна впровадити план оброблення ризиків ІБ.

Організація повинна зберігати задокументовану інформацію стосовно результатів оброблення ризиків ІБ [2].

Створення умов для забезпечення надійного функціонування СМІБ

План перевірок, що проводяться керівництвом

Необхідні дії

Необхідно розробити план, який забезпечуватиме участь керівництва, видачу доручень на перевірку роботи СМІБ та проведення удосконалень.

Вихідні дані:

а) об'єднання всіх областей дії і меж для отримання області дії і кордонів – визначення області дії і кордони СМІБ;

б) розробка політики СМІБ і отримання схвалення керівництва – політика СМІБ;

в) отримання санкції керівництва на впровадження та використання СМІБ – декларація про можливість застосування, включаючи цілі, вибрані заходи, засоби контролю і управління;

г) розробка політики ІБ;

д) вимірювання СМІБ.

Перевірка керівництвом дій із впровадження СМІБ повинна починатися на самих ранніх стадіях складання умов для СМІБ і створення опису застосування СМІБ для даного підприємства і тривати аж до регулярних перевірок операцій СМІБ. Ця безпосередня

Галактика ЕАМ (Enterprise Asset Management) – сучасна інформаційна система управління виробничими активами, заснована на передових методиках обслуговування з орієнтацією на надійність. Галактика ЕАМ дозволяє реалізувати моніторинг технічного стану обладнання та на основі системи критеріїв визначати аварійні об'єкти, що вимагають обслуговування і ремонту [18].

Система дозволяє враховувати всі операції з основними фондами, від закупівлі й монтажу до списання та утилізації. Реалізована можливість зберігати всю інформацію по кожній одиниці обладнання: паспортні дані, всю історію проведених робіт, необхідну документацію і креслення, гарантійні зобов'язання, графік ремонту обладнання та профілактичних робіт, проведення інспекцій, дані про постачальників і виробників запасних частин. У разі запровадження ЕАМ-системи у всіх учасників процесу управління основними фондами з'являється єдине розуміння, чим і як вони керують.

У системі доступний багатофункціональний каталог об'єктів ремонту, представлений вигляді картотеки. У ній міститься інформація про об'єкти ремонту, в картках яких зосереджена вся інформація про виробничі активах підприємства.

У картці об'єкта ремонту обов'язково вказуються основні характеристики самого об'єкта. Так само тут можна відобразити фотографії об'єкта, схеми та інші документи відносяться до активу.

Функціональний склад і можливості системи [12]:

- облік виробничих активів підприємства;
- нормування обслуговування та ремонту обладнання;
- облік стану та експлуатації обладнання;
- облік напрацювання;
- планування робіт;
- розрахунок планових термінів робіт;
- представлення графіків робіт;
- облік запчастин і матеріалів;
- облік виконання робіт;
- аналітичні звіти;
- архів технічної документації;
- процесний підхід управління;

інтерфейсом, що допомагає планувальникам більш ефективно складати і коригувати календарні плани.

Система контролю параметрів ENERGY STAR – модуль, що дає змогу з мінімальними зусиллями складати й вести рейтинги будівель та обладнання для скорочення адміністративних витрат одночасно з безперервною оптимізацією виконання екологічних програм.

Управління автопарком і транспортом – новий модуль управління профілактичним обслуговуванням і технічними роботами, що дозволяє підвищити ефективність превентивного і планового технічного обслуговування автопарку та інших транспортних засобів.

Інтерфейси Infor EAM Connectors – стандартні модулі для організації взаємодії EAM з іншими додатками Infor ERP для скорочення витрат на інтеграцію та забезпечення можливості підключення пристроїв збору даних у режимі реального часу, що дозволяють із мінімальними витратами проводити програми профілактичного та планового обслуговування, а також заходи щодо зниження енергоспоживання.

Лінійні активи – додатковий модуль підтримки декількох схем ESRI, що допомагають підвищити продуктивність праці персоналу і перегляд активів, а також скоротити витрати на інформаційні технології.

Рішення Infor EAM доступне англійською, бразильською, португальською, нідерландською, французькою, німецькою, італійською, японською, спрощеною китайською та іспанською мовами.

Використання рішення Infor10 EAM дозволяє компаніям скоротити простої устаткування і відповідні витрати, а також витрати на технічне обслуговування та ремонти. Рішення надає особливі можливості для стратегічного управління виробничими активами підприємства і допомагає запобігати виходу обладнання з ладу. Крім того, застосування Infor10 EAM забезпечує оптимізацію капітальних витрат, а також дозволяє створювати культуру командної роботи в компанії. Властивість накопичення системою необхідних даних допомагає співробітникам приймати більш раціональні рішення, засновані на повній інформації [17].

Досвід автоматизації управління виробничими активами і процесами ТОіР на промислових підприємствах несе в собі система Галактика EAM.

участь є засобом підтвердження відповідності СМІБ потребам підприємства і підтримки зв'язку підприємства з СМІБ.

Планування перевірок, що проводяться керівництвом, включає встановлення часу і способу проведення перевірок. Щоб запланувати перевірку, необхідно визначити, які посадові особи повинні в ній брати участь. Призначені посадові особи повинні бути затверджені керівництвом і проінформовані про це якомога раніше. Рекомендується надавати керівництву відповідні дані, що стосуються необхідності і мети проведення процесу перевірки.

Перевірки, проведені керівництвом, повинні гуртуватися на результатах вимірювань СМІБ та іншої інформації, накопиченої за час використання СМІБ. Ця інформація використовується для виконання дій керівництвом СМІБ з визначення готовності та ефективності СМІБ. Також слід зазначити, що ці перевірки повинні включати перевірки методології та результатів оцінювання ризику. Перевірки повинні проводитися із запланованим інтервалом з урахуванням зміни середовища, наприклад, організації і технології.

Планування внутрішнього аудиту СМІБ має виконуватися для того, щоб мати можливість регулярно оцінювати СМІБ у міру її впровадження. Результати внутрішнього аудиту СМІБ є важливими вихідними даними для перевірок СМІБ, що проводяться керівництвом. Таким чином, до проведення перевірки керівництвом необхідно запланувати внутрішній аудит. Внутрішній аудит СМІБ повинен включати перевірку того, чи ефективно впроваджуються і зберігаються цілі, заходи і засоби контролю й управління, процеси і процедури СМІБ і чи відповідають вони:

а) вимогам ISO / IEC 27001;

б) з чинним законодавством і правилами;

в) певним вимогам до ІБ.

Попередньою умовою для проведення перевірок керівництвом є інформація, зібрана на основі впровадженої і використовуваної СМІБ. Інформація, яку надає групі керівників, які проводять перевірку, може включати наступне:

а) звіти про інциденти за останній період використання системи;

б) підтвердження ефективності управління та виявлені невідповідності;

в) результати інших регулярних перевірок (більш докладні, якщо під час перевірки були виявлені невідповідності з політикою ІБ);

г) рекомендації щодо вдосконалення СМІБ.

У плані моніторингу повинні документуватися його результати, які повинні записуватися і повідомлятися керівництву.

Вихідні дані

Вихідними даними цієї дії є документ, що містить план, необхідний для організації перевірок, що проводяться керівництвом:

а) вихідні дані, необхідні для перевірки СМІБ керівництвом;

б) процедури перевірок, що проводяться керівництвом і стосуються аспектів аудиту, моніторингу та вимірювання.

Розробка програми інформування, навчання та освіти у сфері інформаційної безпеки

Необхідні дії

Необхідно розробити програму інформування, навчання та освіти в області ІБ.

Вихідні дані:

а) об'єднання всіх областей дій і меж для отримання області дії і кордонів – область дії і кордони СМІБ;

б) розробка політики СМІБ і отримання схвалення керівництва – політика СМІБ;

в) визначення вимог до ІБ для процесу СМІБ;

г) отримання санкції керівництва на впровадження та використання СМІБ – декларація про можливість застосування, включаючи цілі, обрані заходи і засоби контролю та управління;

д) вибір цілей і засобів управління – План обробки ризику;

е) розробка політики ІБ;

ж) розробка стандартів і процедур забезпечення ІБ;

з) огляд загальної програми освіти та навчання в організації.

Керівництво відповідає за освіту і навчання, щоб співробітники, призначені на певні посади, мали необхідні знання для виконання необхідних операцій. В ідеалі зміст програми освіти та навчання має допомагати всім співробітникам знати й розуміти значення і важливість операцій щодо забезпечення ІБ, в яких вони беруть участь, і те, як вони можуть сприяти досягненню цілей.

На цьому етапі важливо забезпечити, щоб кожен працівник у межах сфери дії СМІБ отримав необхідне навчання та (або) освіту.

час. Оновлений EAM-додаток від Infor заснований на сучасних мобільних технологіях, що дозволяють застосовувати його в будь-який час в будь-якій точці світу за допомогою Інтернет з використанням смартфонів, IT-планшетів та інших мобільних пристроїв. Крім того, рішення Infor10 EAM може бути розгорнуто як на локальному обладнанні, так і з використанням хмарної технології Infor10 Cloud Suite. При цьому можливо й одночасне розміщення даних частково локально і частково як SaaS-додаток, надаючи користувачам максимальну гнучкість у розгортанні EAM-системи [16].

Рішення Infor10 EAM володіє сучасними функціями та властивостями, особливо цінними для безпосередніх користувачів. Раціонально структурований старт-центр, що враховує рольову належність співробітника, а також можливість відображення статусу цікавлять конкретного користувача бізнес-процесів забезпечують зручне застосування програмного програми. Завдяки надходженню в EAM-систему даних про стан об'єктів основних фондів і різних процесів в рамках підприємства в режимі реального часу рішення Infor10 EAM надає цілісну картину актуальної інформації про компанію «зсередини». Рішення також включає широкі аналітичні можливості для виявлення, пріоритезації та попередження ризиків, критичних для бізнесу [16].

EAM-рішення від Infor на базі платформи Infor10, легко інтегрувальне в корпоративну IT-інфраструктуру, традиційно включає передову функціональність з управління життєвим циклом капітальних активів, матеріально-технічним постачанням, роботами, трудовими ресурсами, лінійними об'єктами, загальною продуктивністю, енергоефективністю, ризиками і надійністю обладнання. Рішення має важливою функціональністю з формування аналітичних даних, а також звітності різних рівнів складності. Використання рішення Infor10 EAM дозволяє компаніям скоротити простої устаткування і відповідні витрати, а також витрати на технічне обслуговування й ремонти [17].

У рішенні Infor10 EAM розширені й додані такі функції:

Графічна панель планування розкладів – зручна система для управління ресурсами з широким набором фільтрів для перегляду даних за кілька тижнів, наочними індикаторами стану і графічним

мають відношення до процесів управління, ремонту та обслуговування активів, можуть виконувати свої функції більш ефективно, скорочуючи обсяг витрат на обслуговування та ремонт активів підприємства.

Використовуючи систему Maximo, користувач отримує можливість побачити всі активи підприємства зсередини, подивитися, як функціонує обладнання, основні системи, побачити, де і за рахунок чого можна мінімізувати витрати, які перешкоджають збільшенню прибутку, зростання продуктивності. Можна швидко одержувати консолідовану інформацію, що надходить з найвіддаленіших підрозділів організації і у разі необхідності деталізувати цю інформацію до рівня активу, запчастин, матеріалів, досліджуючи й аналізуючи свій бізнес, знаходячи шляхи й можливості для його поліпшення та усунення наявних проблем [7].

Інша з найбільш поширених та відомих систем є **Infor10 EAM Asset Sustainability**. Дана система пропонує більш досконале рішення з управління активами, оскільки існуючі системи не вирішують навіть поточних проблем, не говорячи вже про потенційні майбутні проблеми. Досягти цільових показників із використанням традиційних систем управління активами неможливо, тому що вони не дозволяють враховувати одну з найважливіших статей витрат, що відносяться до основних засобів, – енергію. Важливо те, що енергоефективність, як основний показник ефективності основних засобів, може стати ключовим фактором в процесі досягнення цілей компанії щодо експлуатаційної готовності й надійності активів.

Infor10 EAM призначена для вирішення найскладніших задач профілактичного обслуговування активів в дискретному виробництві і компаніях харчового сектору, управління енерговитратами в целюлозно-паперовому секторі, облік ризиків в медицині, управління парком техніки в транспортних компаніях, контролю лінійних активів у нафтогазовому секторі, моніторингу основних засобів і їх обслуговування залежно від технічного стану в державних організаціях і для багатьох інших цілей [15].

Infor10 EAM володіє всіма унікальними перевагами рішень компанії Infor сімейства Infor10. Зокрема, воно наділене ультрасучасним інтерфейсом Workspace, що дає користувачам можливість бачити на екрані важливу саме для них інформацію в потрібний

У великих організаціях одного набору матеріалів з навчання, як правило, недостатньо, оскільки він повинен містити занадто багато даних, що відносяться тільки до окремих типів робіт, і, отже, буде великим, складним і важким у використанні.

У таких випадках зазвичай рекомендується мати різні набори матеріалів з навчання, розроблених для різних груп ролей, наприклад, офісних працівників, які обслуговують працівників або керівників в області ІТ, які забезпечують конкретні потреби цих працівників.

Програма навчання й освіти з метою інформування з питань ІБ повинна забезпечувати складання записів з навчання й освіти в галузі ІБ. Ці записи повинні регулярно перевірятися для забезпечення отримання необхідного навчання усіма співробітниками. Необхідно призначити посадову особу, відповідальну за цей процес.

Матеріали з навчання в області ІБ повинні бути розроблені таким чином, щоб вони були пов'язані з іншими навчальними матеріалами, використовуваними в організації, особливо навчальні курси для користувачів ІС. Навчання за істотними аспектам ІБ в ідеалі повинно включатися в кожен навчальний курс для користувачів ІТ.

Навчальні матеріали з ІБ повинні включати як мінімум такі пункти в залежності від цільової аудиторії:

– ризики і загрози, пов'язані з ІБ;
– основні терміни з ІБ;
– чітке визначення інциденту безпеки: рекомендації з виявлення інциденту, його усунення та звітності;
– політики ІБ, стандарти і процедури організації;
– сфери відповідальності і канали звітності, пов'язані з ІБ в організації;
– рекомендації з надання допомоги у підвищенні ІБ;
– рекомендації, пов'язані з порушеннями ІБ і звітністю;
– де отримати додаткову інформацію.

Необхідно визначити групу з навчання ІБ, яка може виконувати наступні завдання:

а) створення і управління записами з ІБ;
б) складання і управління матеріалами з навчання;
в) проведення навчання.

Ці завдання можуть ставитися з урахуванням використання існуючого навчального персоналу. Але для існуючого персоналу може знадобитися навчання концепціям ІБ, щоб забезпечити їх ефективне й точне уявлення.

Програма інформування, освіти та навчання у сфері ІБ повинна включати процедуру, що забезпечує регулярну перевірку й оновлення навчальних матеріалів.

Для перевірки та оновлення навчальних матеріалів можна призначити спеціальне посадова особа.

Вихідні дані

Вихідні дані цього дії наступні:

а) матеріали з інформування, навчання і освіти в області ІБ;

б) формування програм інформування, освіти та навчання в області ІБ, включаючи ролі та сфери відповідальності;

в) плани інформування, освіти та навчання в галузі ІБ;

г) актуальні записи, що показують результати інформування, освіти та навчання працівників у сфері ІБ [3].

2.8. Оцінка ефективності СМІБ

Моніторинг, вимірювання, аналіз та оцінювання

Організація повинна оцінювати результативність ІБ та ефективність СМІБ.

Організація повинна визначити:

а) що саме потрібно моніторити й вимірювати, включаючи процеси ІБ та заходи безпеки;

б) методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;

в) коли моніторинг та вимірювання потрібно виконувати;

г) хто повинен виконувати моніторинг та вимірювання;

д) коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати;

е) хто повинен аналізувати й оцінювати ці результати.

Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

Внутрішній аудит

Організація повинна проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи СМІБ:

класу ERP (наприклад, SAP) Maximo являє собою закінчене «вертикальне» рішення, яке доповнює ERP і охоплює всі рівні управління підприємством: від виробничо-технологічного до фінансово-економічного [7].

До складу розширеної сервіс – орієнтованої архітектури Maximo Asset Management входить шість модулів управління [14]:

Управління активами – усі функції та інструменти, необхідні для ретельного відстеження та ефективного управління даними про корпоративні активи та їх розміщення протягом всього їх життєвого циклу.

Управління роботами – управління роботами з плановому й позаплановому обслуговуванні активів – від генерації заявок і нарядів на проведення робіт до реєстрації фактично здійснених заходів.

Управління обслуговуванням – визначення пропозицій з обслуговування, встановлення угод про рівень обслуговування, більш активне відстеження рівня наданих послуг та впровадження процедур ескалації.

Управління договорами – забезпечення повної підтримки договорів купівлі – продажу, оренди, лізингу, гарантійних, трудових договорів, договорів на поставку програмного забезпечення, головних/групових договорів, комплексних договорів, а також специфічних видів договорів, визначених користувачем.

Управління матеріальними запасами – доступ до повної інформації про матеріальні запаси, що пов'язані з активами і їх використання.

Управління закупівлями – підтримка всіх операцій постачання в масштабах підприємства, включаючи прямі закупівлі й поповнення товарно-матеріальних запасів.

Система Maximo є платформенно незалежною, використовує передові веб-рішення й побудована з використанням технології «тонкого» клієнта. Maximo об'єднує традиційний EAM-підхід до управління виробничими активами підприємства з методологією ITSM, що дає змогу ефективно управляти всім спектром стратегічних активів підприємства, включаючи виробничі потужності, будівлі та споруди, транспортний парк та IT-активи [7].

За допомогою цього спеціалізованого продукту керівники підприємства, головний інженер, співробітники служби ремонту та обслуговування активів, співробітники всіх інших підрозділів, що

Рис. 4.13. Повний життєвий цикл активу

Система **IBM Maximo** являє собою єдине рішення для управління всіма типами активів – виробничих, транспортних, інфраструктурних, комунальних ресурсів, будівель і споруд, а також IT-активів. IBM – перша компанія з постачальників рішень інтегрувала на єдиній платформі продукти для управління всіма можливими типами активів, вписавши їх у контекст управління сервісами.

Фактично IBM пропонує своїм замовникам зручний конструктор, з якого конкретна організація може побудувати необхідне їй середовище управління активами, вибираючи відповідні модулі й налаштовуючи потрібні процеси. Простота складання і розширення такого середовища є ще однією відмінною особливістю системи IBM [14].

У кожній сучасній організації є активи, що роблять дуже впливають на ефективність і прибутковість її основних бізнес-процесів. Грамотно керуючи і оптимізуючи процеси обслуговування активів, компанія розвиває конкурентні переваги, відкриває приховані раніше можливості збільшення власної прибутковості.

IBM Maximo Asset Management (Maximo) – одне з найкращих рішень серед систем класу EAM, що автоматизує процеси управління експлуатацією, технічним обслуговуванням і ремонтами технологічного устаткування, об'єктів транспортної, виробничої інфраструктури підприємства.

Відмінною особливістю Maximo в порівнянні з іншими системами подібного класу є розширена функціональність управління сервісами та сервісними відносинами. В інтеграції з системами

а) відповідають

1) власним вимогам організації для її СМІБ;

2) вимогам цього стандарту;

б) ефективно впроваджена та підтримується.

Організація повинна:

а) планувати, розробляти, впроваджувати та підтримувати програму(-и) аудиту, зокрема й частоту, методи, відповідальності, заплановані вимоги та звітність. Програма(-и) аудиту повинна(-і) враховувати аналіз важливості процесів, що їх розглядають, і результати попередніх аудитів;

б) визначити критерії аудиту та сферу застосування для кожного аудиту;

в) призначити аудиторів і виконати аудити, які гарантують об'єктивність і неупередженість процесу аудиту;

г) гарантувати, що результати аудиту буде доведено до відповідного керівництва;

д) зберігати документовану інформацію як доказ програми аудиту та результатів аудиту.

Перегляд з боку керівництва

Вище керівництво повинно переглядати СМІБ організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності.

Перегляд з боку керівництва повинен стосуватися розгляду:

а) статусу дії, що є наслідком попереднього перегляду керівництва;

б) зміни в зовнішніх та внутрішніх обставинах, які мають відношення до СМІБ;

в) зворотного впливу на результативність ІБ, охоплюючи тенденції в:

1) невідповідностях та коригувальних діях;

2) результатах моніторингу та вимірювань;

3) результатах аудиту;

4) досягненнях цілей ІБ;

г) зворотного зв’язку від зацікавлених сторін;

д) результатів оцінювання ризиків і статусу плану оброблення ризиків;

е) можливостей для постійного вдосконалення.

Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до СМІБ.

Організація повинна зберігати документовану інформацію як доказ результатів переглядів з боку керівництва [2, 6].

Питання оцінки ефективності СЗІ від НСД:

1) Оцінка коректності реалізації механізмів захисту СЗІ від НСД. На практиці провести таку оцінку є досить важким завданням. Оскільки можливий варіант, коли встановлена у ІС СЗІ від НСД не перехоплює і не аналізує лише один подібний спосіб звернення до файлового об'єкту, і, за великим рахунком, вона стає цілком даремною (рано чи пізно, зловмисник виявить даний недолік засобів захисту і скористається ним). Звідси отримуємо вимогу до коректності реалізації СЗІ від НСД – вона повинна контролювати доступ до ресурсу за будь-якого способу звернення до ресурсу (ідентифікації ресурсу).

2) Оцінка достатності (повноти) набору механізмів захисту у складі СЗІ від НСД. Тут ситуація багато в чому схожа із ситуацією, описаною вище. Наприклад, вимога до достатності механізмів у СЗІ від НСД для захисту конфіденційних даних у нормативних документах виглядає наступним чином: «Чи повинен здійснюватися контроль доступу суб'єктів до ресурсів, що захищаються відповідно до матриці доступу». Природно виникає неоднозначність визначення того, що віднести до ресурсів, які захищаються? Крім того, необхідно розуміти, що безліч комп'ютерних ресурсів (особливо, коли мова йде про універсальну операційну систему (ОС)) для корпоративних додатків зайві, в першу чергу, це стосується всіляких зовнішніх пристроїв. На думку фахівців, об'єктивним видом оцінки ефективності СЗІ є функціональне тестування, призначене для перевірки фактичної працездатності реалізованих механізмів безпеки та їх відповідності висунутим вимогам, а також гарантування отримання статистичних даних [7]. У силу того, що засобам безпеки властиві обмежені можливості з протидії загрозам, завжди існує імовірність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї ймовірності повинні проводитися додаткові дослідження.

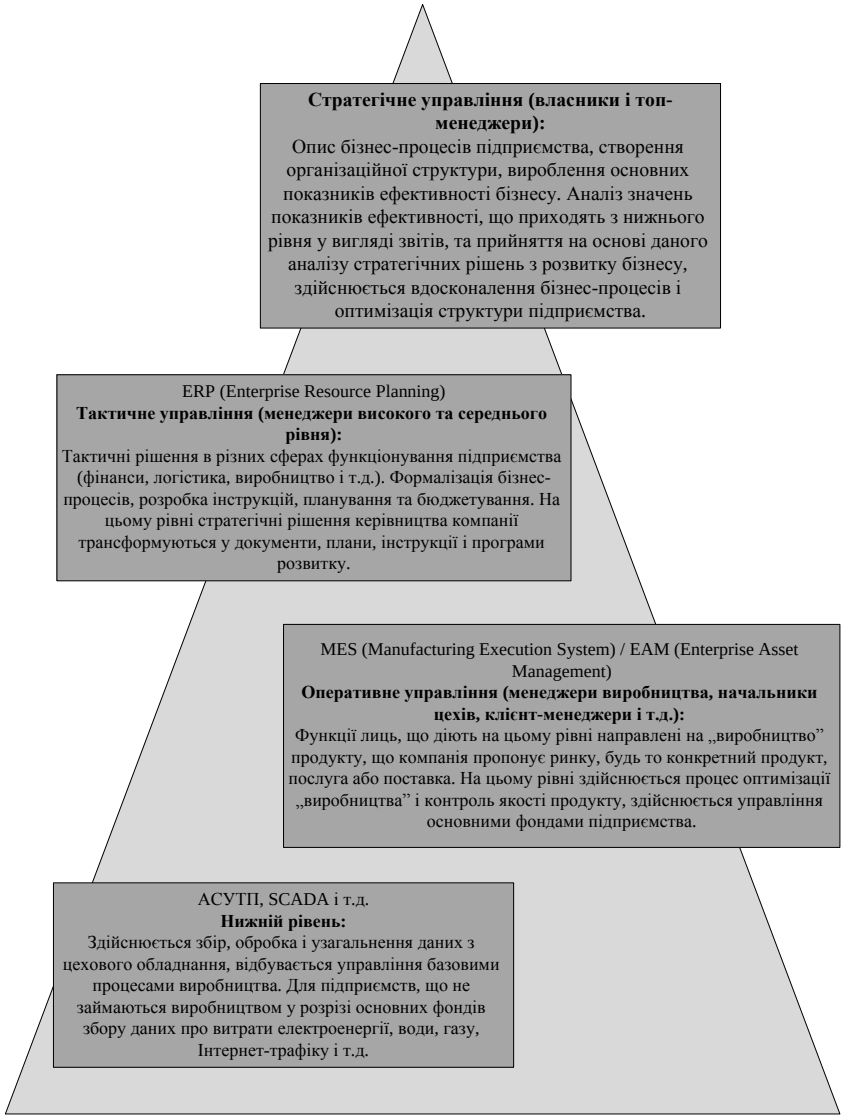


Рис.4.12. Позиціонування систем класу EAM

EAM-системи допомагають узгоджено керувати наступними основними процесами, що відносяться до обслуговування і ремонту активів підприємства.

Подання системи управління підприємством у вигляді піраміди, розділеної на рівні, стало вже класичним. Вершина піраміди – це рівень прийняття стратегічних рішень, під ним лежить рівень тактичного управління, далі йде рівень оперативного управління, і спирається вся система на низовий рівень (рис. 4.12).

Окремим класом на рис. 4.12 виділені системи, що відповідають за рівень оперативного управління, системи класу **MES** (Manufacturing Execution System). Чому? Відповідь гранично проста – попри всі запевнення розробників, ERP-системи не дозволяють відслідковувати безпосередньо виробництво з тим ступенем деталізації та оперативності, яка може дати компанії дійсно корисну інформацію, зробить виробництво прозорим і керованим. Крім того, ERP-системи не розраховані на пряму інтеграцію з АСУТП для отримання первинних даних, що знижує їх придатність до управління виробництвом. Якщо говорити про підприємство, яке надає послуги, що займається дистрибуцією і т.ін., то ERP-система, безумовно, забезпечить обидва рівня тактичного та оперативного управління, але на виробничому підприємстві без MES-системи вже не обійтися [12].

Останній низовий рівень управління підприємства зазвичай реалізується системами АСУТП, SCADA тощо залежно від завдань, що стоять перед підприємством. Усі провідні ERP-системи мають модуль управління основними фондами. Управління основними фондами є однією з 11 узагальнених функцій MES-системи, які визначила міжнародна асоціація виробників систем управління виробництвом (MESA).

EAM-система – це повноцінний управлінський облік, з яким працюють менеджери, що безпосередньо відповідають за стан активів, причому не тільки верхньої і середньої ланки, а й молодші керівники (бригадири, майстри, прості робітники) [13].

EAM-система – це повністю інтегроване прикладне програмне забезпечення управління основними фондами підприємства в рамках стратегії EAM. Варто відзначити, що EAM-системи допомагають керувати повним життєвим циклом активу, починаючи з його проектування/купівлі і закінчуючи списанням (рис.4.13) [13].

У методичному плані визначення ефективності СЗІ має полягати у виробленні судження щодо придатності способу дій персоналу або пристосованості технічних засобів до досягнення мети захисту інформації на основі вимірювання відповідних показників, наприклад, при функціональному тестуванні.

Ефективність оцінюється для вирішення наступних завдань:

– прийняття рішення про допустимість практичного використання СЗІ в конкретній ситуації;

– виявлення внесків різних факторів у досягнення мети;

– встановлення шляхів підвищення ефективності СЗІ;

– порівняння альтернативних варіантів систем.

Таким чином, при використанні сучасної методичної бази, оцінка ефективності СЗІ носить, в основному, нечіткий, суб'єктивний характер. Практично повністю відсутні нормовані кількісні показники, що враховують можливі випадкові чи навмисні дії. У результаті досить складно, а часто і неможливо, оцінити якість функціонування ІС за наявності несанкціонованих впливів на її елементи, а, відповідно, і визначити, чим один варіант проектованої системи краще іншого. Можливим вирішенням проблеми комплексної оцінки ефективності СЗІ є використання системного підходу, що дозволяє ще на стадії проектування кількісно оцінити рівень безпеки та створити механізм управління ризиками. Але цей шлях реалізується за наявності відповідної системи показників і критеріїв.

Існують наступні методи та засоби оцінки ефективності СЗІ:

1) Метод порівняльного багатовимірного аналізу. Цей метод створений для визначення ступеня взаємного впливу загроз та причин їх виникнення (і як результат – оцінка ефективності СЗІ). Суть методу можна звести до такого узагальненого алгоритму:

– складається перелік об’єктів, що оцінюються, і вибираються ознаки, за якими буде проводитись оцінка. В даному випадку під об’єктами оцінки будемо розуміти показники захищеності обчислювальної системи, а під ознаками – сукупність параметрів, що характеризують ці показники;

– цей перелік слугує основою для формування матриці ознак $X(n, w)$, де n – кількість ознак, а w – кількість об’єктів, що оцінюються. Кожному об’єкту ставиться у відповідність рядок матриці із n ознак;

– через те, що дані, які зведені в матрицю, описують різні властивості об’єктів і мають різні одиниці виміру, вихідна матриця нормалізується відповідно до формули

$$Z_{ik} = \frac{x_{ik} - \overline{x_k}}{s_k},$$

де $\overline{x_k} = \frac{1}{w}\sum_{i=1}^{w} x_{ik}$ – середнє арифметичне ознаки k по усіх об’єктах,

$s_k = \left[\frac{1}{w}\sum_{i=1}^{w}(x_{ik} - \overline{x_k})^2\right]^{\frac{1}{2}}$ – стандартне відхилення ознаки k; Z_{ik} – нормалізоване значення ознаки k для одиниці об’єкта i;

– проводиться розрахунок елементів матриці відстаней між показниками захищеності з урахуванням усіх елементів матриці ознак: $W_{rs} = \frac{1}{n}\sum_{k=1}^{n}|z_{rk} - z_{sk}|, r, s = \overline{1, w}.$

По отриманій матриці відстаней між показниками здійснюються їх зіставлення між собою, яке дає змогу впорядкувати показники за ступенем важливості, встановити залежності між ними, оцінити ступінь їх взаємного впливу. З використанням цього методу можна провести порівняльний аналіз загроз інформації та причин, які впливають на їх виникнення, кількох комп’ютерних мереж, що експлуатуються, наприклад, в державних установах. Для формування матриці ознак використовувався метод експертного опитування посадових осіб, до компетенції яких входить адміністрування (як технічне, так і організаційне) комп’ютерних мереж. Під час такого опитування адміністраторам комп’ютерних мереж пропонувалося заповнити анкету, в якій були перелічені загрози інформації та причини їх виникнення, шляхом визначення пріоритету кожної з них за десятибальною шкалою. Головною вимогою при заповненні анкети було врахування конкретних умов експлуатації комп’ютерної мережі. Обробка результатів опитування відповідно до викладеної вище методики дала змогу оцінити взаємний вплив існуючих загроз і скоригувати відповідним чином політику ЗІ.

2. Методи аналізу ризиків інформаційних систем (ІС). На даний час при побудові СЗІ особливого значення набуває завдання побу-

жують виконуватися задовільно. Для аудиту стандарт пропонує набір питань, на які необхідно відповісти, щоб визначити: чи потрібні внести які-небудь зміни в RCM-процес, реалізований на підприємстві [7].

Стандарт ISO 27001 визначає процеси, що дають можливість бізнесу встановлювати, застосовувати, переглядати, контролювати й підтримувати ефективну СМІБ, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої СІМБ у контексті наявних бізнес ризиків організації.

Аналіз наявних систем управління активами підприємства.

Старіння активів, тяжкі умови праці, посилення нормативних вимог і жорстока ринкова конкуренція змушують застосовувати в роботі підприємства систему з управління активами. На сьогодні на ринку запропоновано чималу кількість розроблених систем управління активами підприємства, що спеціалізуються на безлічі різновидів активів, в основу деяких покладено стратегію EAM.

У кожній сучасній організації є активи, що справляють значний вплив на ефективність і прибутковість її основних бізнес-процесів. Грамотно керуючи й оптимізуючи процеси обслуговування активів, компанія розвиває конкурентні переваги, відкриває приховані раніше можливості збільшення власної прибутковості.

Enterprise Asset Management (EAM) – це систематична і скоординована діяльність організації, спрямована на оптимальне управління фізичними активами і режимами їхньої роботи, ризиками й витратами протягом усього життєвого циклу для досягнення і виконання стратегічних планів організації. Зауважимо, що реалізація стратегії EAM безпосередньо пов'язана з технічним обслуговуванням і ремонтами (TOiP) – життєво важливою областю діяльності індустріальних, видобувних, енергетичних і транспортних компаній, а також операторів зв'язку [10].

Системи класу EAM – інтегровані системи управління основними фондами є логічним розвитком комп'ютерних систем управління ремонтами (Computerized Maintenance Management Systems – CMMS), які існують уже більше 20 років. Основне призначення CMMS-систем – це скорочення витрат на обслуговування обладнання і підвищення продуктивності (коефіцієнта готовності). Навпаки, основна мета застосування EAM-систем – стратегічна і полягає в мінімізації витрат підприємства [11].

6) Визначити, що потрібно вжити для попередження кожної відмови.

7) Визначити ефективні способи обслуговування для даного обладнання.

Ці способи обслуговування в стандарті названі «політиками управління відмовами», і мова йде про застосовність і ефективність тієї чи іншої політики для даного обладнання. Наприклад, якщо тяжкість наслідків відмови невисока, то буде неефективно використовувати дорогі методи попереджувального обслуговування. Тут може бути доцільним відновлення після відмови – тобто політика, яка дозволяє певному виду відмови відбутися без будь-яких спроб його запобігання [7].

Стандарт JA 1012 «Керівництво до RCM-стандарту» описує два підходи до вибору політик управління відмовами [9]:

– строгий підхід – є більш повним;

– діаграми прийняття рішень – більш простий, дешевий і популярний.

Строгий підхід до вибору політик управління відмовами, вимагає оцінювати економічні наслідки і наслідки, пов'язані з безпекою та екологією, для кожного виду відмови.

Діаграми засновані на припущенні, що насамперед необхідно розглядати загрози безпеки/екології і тільки після цього економічні наслідки. Друге припущення – що деякі категорії політик управління відмовами завжди більш ефективні економічно. На цій основі політики управління відмовами зводяться в ієрархії, які допомагають здійснити вибір.

Після усвідомленого вибору політик управління відмовами формується довгострокова програма робіт для кожного окремого активу, або для системи активів. Ця програма надалі служить основою при формуванні план-графіку робіт на період (рік, квартал і т. ін.), з якого вже слідують завдання на роботу для виконавців, потреби в матеріально-технічних ресурсах, плани закупок МТР і так далі.

Стандарт JA 1012 встановлює, що будь-який RCM-процес повинен підлягати періодичному аудиту як з погляду інформації, використовуваної при прийнятті рішень, так і щодо самих рішень. Аудит повинен гарантувати, що всі зазначені вище сім етапів продов-

дови моделей загроз інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків ІС [8].

2.9. Вдосконалення СМІБ

Невідповідності й корегувальні дії

У разі виявлення невідповідностей організація повинна:

а) реагувати на невідповідності і за можливості:

1) виконувати дії для контролю та їх корекції;

2) вживати заходів щодо наслідків;

б) оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою:

1) перегляду невідповідностей;

2) визначення причин невідповідностей;

3) визначення, чи існують подібні невідповідності або потенційно можуть з’являтися;

в) впровадити певні дії, за потреби;

г) переглянути ефективність виконаних коригувальних дій;

д) внести зміни до СМІБ, за потреби.

Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей. Організація повинна зберігати документовану інформацію як доказ:

е) сутності невідповідностей та будь-яких послідовних дій, що були виконані,

ж) результати будь-яких коригувальних дій.

Постійне вдосконалення

Організація повинна постійно вдосконалювати придатність, адекватність та ефективність СМІБ, гарантування її постійної придатності, адекватності та ефективності [6].

За результатами внутрішнього аудиту СМІБ і аналізу з боку керівництва розробляються і впроваджуються коригувальні та запобіжні дії, спрямовані на постійне поліпшення СМІБ:

а) Удосконалення політики ІБ, цілей ЗІ, проведення аудиту, аналіз спостережуваних подій.

б) Розробка і реалізація коригувальний і застережливих дій для усунення невідповідностей СМІБ вимогам.

в) Контроль поліпшень СМІБ.

Питання для самоконтролю

1) Які переваги можуть бути від впровадження СМІБ на підприємстві?
2) Що таке рейдерство?
3) Як визначається місце та область поширення СМІБ в організації?
4) Що спільного між системою менеджменту якості та СМІБ?
5) Наведіть п’ять фаз планування кінцевого впровадження СМІБ?
6) Що таке контекст організації?
7) Як реалізується оцінка ефективності СМІБ?

оптимізацію використання ресурсів за критерієм максимуму надійності в умовах діючих ресурсних та інших обмежень [7].

Опис RCM вперше було опубліковано Міністерством оборони США. Відтоді RCM стала широко застосовуватися в більшості галузей індустрії в багатьох країнах. Процес, визначений у описі, став використовуватися як основа для розробки та вдосконалення RCM-процесу в різних документах, що застосовуються компаніями. Багато з таких документів зберігають ключові елементи RCM.

Однак широке використання RCM призвело до того, що з'явилося багато варіантів, які разюче відрізняються від оригіналу. Так виникла необхідність у створенні міжнародного стандарту, який би встановлював критерії відповідності того чи іншого процесу, застосовуваного для вибору стратегії обслуговування, певним вимогам, званим «RCM». Такий стандарт був створений Society of Automotive Engineers (SAE), у двох частинах, і отримав назву SAE JA 1011:2009 і JA 1012:2011

Стандарт SAE JA 1011 «Критерії для оцінки процесу управління надійністю» містить мінімальні вимоги до процесу RCM. Критерії, що містяться в ньому, базуються безпосередньо на концепції, запропонованої авторами опису RCM, та інших роботах.

Документ SAE JA 1011 призначений для використання під час оцінювання – наскільки розглянутий процес відповідає споконвічно закладеним принципам RCM. Документ корисний для тих, кому потрібні послуги з впровадження RCM.

Згідно SAE JA 1011, будь-який процес, щоб він вважався RCM-процесом, повинен містити всі перераховані нижче етапи в зазначеній послідовності [9]:

1) Визначити особливості умов експлуатації обладнання і виконуваних ним функцій, а також пов'язані з ними номінальні характеристики продуктивності.
2) Визначити, як обладнання може припинити виконувати свої функції (функціональні відмови).
3) Визначити причини кожної функціональної відмови (види відмови).
4) Визначити, що саме відбудеться при кожній відмові (наслідки відмови).
5) Класифікувати значимість наслідків відмови (тяжкість наслідків відмови).

– організаціям, які, у зв'язку з вимогами суспільства або бізнесу, повинні демонструвати найкращі показники у сфері безпечного управління активами і надання пов'язаних з активами послуг (наприклад, підприємства сектора освіти чи охорони здоров'я).

Виконання вимог стандарту PAS 55 дає змогу організації узгодити або інтегрувати її систему управління активами з іншими методиками для досягнення єдиних цілей. Структура і вимоги стандарту організовані відповідно до циклу Демінга PDCA (Plan-Do-Check-Act). Цикл PDCA символізує принцип повторення у вирішенні проблеми – досягнення поліпшення крок за кроком, і повторення циклу вдосконалення багато разів.

Все це дозволяє:

1) Планувати. Розробка стратегії, плану і цілей управління активами, необхідних для досягнення результатів, визначених у політиці управління активами і стратегічному плані організації.

2) Виконувати. Створення умов, необхідних для впровадження управління активами (наприклад, впровадження інформаційної керуючої системи (систем)), а також виконання інших вимог (наприклад, вимог законодавства) і реалізація плану (планів) управління активами.

3) Перевіряти. Відстеження і оцінювання результатів діяльності в порівнянні з вимогами політики, цілей управління активами, вимог законодавства і т. ін.; створення звіту про отримані результати.

4) Впливати. Забезпечення впевненості в тому, що поставлені цілі управління активами виконуються, система управління активами знаходиться в безперервному розвитку, і продуктивність активів із часом підвищується.

Не менш важливим для забезпечення надійного і якісного управління активами є обслуговування, що орієнтоване на надійність, що розглядається стандартами SAE JA 1011, 1012.

Вибір відповідних обґрунтованих методів обслуговування (стратегій обслуговування) – це процес визначення оптимальних програм технічного обслуговування для управління відмовами фізичних активів і систем. У практиці багатьох великих компаній такий підхід застосовується і відомий як Reliability Centered Maintenance (RCM), або система технічного обслуговування, орієнтована на забезпечення надійності. Підхід RCM спрямований на

СПИСОК ЛІТЕРАТУРИ ДО ДРУГОГО РОЗДІЛУ

1) А.А. Дмитриев: «ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях», «Das Management» №1, 2009, с. 36-39.

2) «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

3) «Information technology. Security techniques. Information security management systems implementation guidance», ISO/IEC 27003:2017, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017, p. 45.

4) «IT-Grundschutz Methodology – Community Draft», BSI-Standard 200-2, Federal Office for Information Security (BSI), 2017, p. 131.

5) «Системи забезпечення інформаційної безпеки. Огляд», Компанія «Валтек», 2018. [Online]. Available: https://valtek.com.ua/ua/system- integration/ security-control-system/ integrated- security-systems /information-security-system-review [Accessed: 26- Dec- 2018].

6) «Методи захисту системи управління інформаційною безпекою», Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП «УкрНДНЦ», 2016, с. 28.

7) Д.А. Поспєлов, Нечёткие множества в моделях управления и искусственного интеллекта, М., Наука, 1986, с. 312.

8) О.І. Гарасимчук, Ю. М. Костів, Оцінка ефективності систем захисту інформації, Вісник КНУ імені Михайла Остроградського. Випуск 2 (67), 2011, с. 16-20.

Розділ 3. ПРОЦЕСИ РИЗИК-МЕНЕДЖМЕНТУ

Систематичний підхід до менеджменту ризику ІБ необхідний для того, аби ідентифікувати потреби організації, що стосуються вимог ІБ та створити ефективну СМІБ. Цей підхід повинен бути придатним до середовища організації і, зокрема, повинен підтримувати менеджмент ризиків для всієї організації. Зусилля щодо забезпечення безпеки повинні ефективно і своєчасно розглядати ризики там і тоді, де і коли це необхідно. Менеджмент ризиків ІБ повинен бути невід'ємною частиною всіх видів діяльності, пов'язаних із менеджментом ІБ, а також повинен застосовуватися для реалізації і підтримки функціонування СМІБ організації.

Менеджмент ризику ІБ повинен бути безперервним процесом. Цей процес повинен встановлювати контекст, підтримувати оцінку й обробку ризиків, забезпечувати використання плану обробки ризику для реалізації, сприяти виробленню рекомендацій і рішень. Менеджмент ризику пов'язаний з аналізом того, що може статися, і якими можуть бути можливі наслідки, перш ніж виробити рішення про те, що і коли повинно бути зроблено для зниження ризику до прийнятного рівня.

Менеджмент ризику ІБ повинен сприяти наступному:

- ідентифікації ризиків;
- оцінюванню ризиків (ОР), виходячи з наслідків їх реалізації для бізнесу та ймовірності їх виникнення;
- вивченню ймовірності й потенційних наслідків даних ризиків;
- встановленню порядку пріоритетів в рамках обробки ризиків;
- встановленню пріоритетів заходів щодо зниження ризиків;
- залученню зацікавлених сторін до прийняття рішень про менеджмент ризиків та підтримання їх інформованості про стан менеджменту ризиків;
- ефективності обраного моніторингу обробки ризиків;
- проведенню регулярного моніторингу та переглядання процесу менеджменту ризиків;
- збору інформації для удосконалення підходу до менеджменту ризиків;
- підготовці менеджерів і персоналу в частині управління ризиками і необхідних дій, що вживаються для їх зменшення.

активами є життєво необхідною для організацій, випуск продукції або послуги в яких залежить від працездатності та продуктивності їх фізичних активів. Успіх таких організацій істотно залежить від ефективності управління їх активами.

Є певні спірні фактори, що потребують врахування, таких як вибір між короткостроковими і довгостроковими вигодами, знаходження оптимального співвідношення між витратами та продуктивністю, запланована і фактична доступність активів, або співвідношення капітальних витрат і операційних витрат.

На рис. 4.11 показані рівні систем управління активами, а також напрями оптимізації, що визначаються стандартом PAS 55 [8].

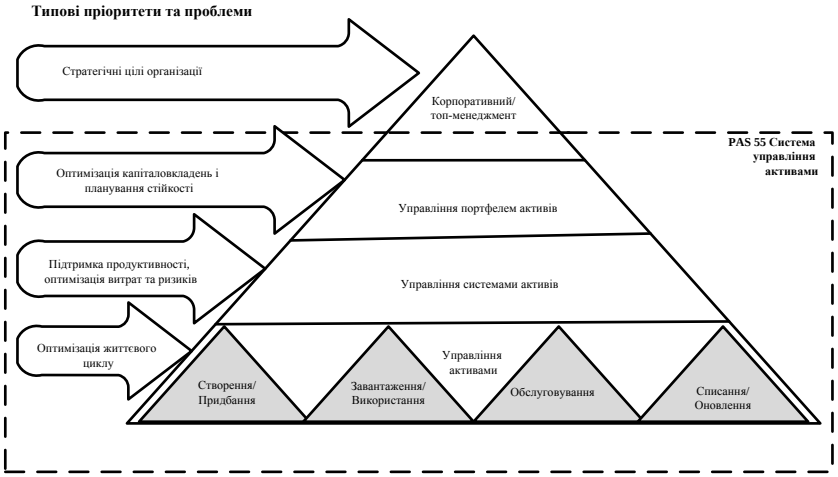


Рис. 4.11. Рівні управління активами

Даний стандарт застосовується для [8]:

- будь-якого підприємства, яке інтенсивно використовує активи, в якому витрати, ресурси, продуктивність і/або ризики пов'язані із створенням/придбанням, використанням, обслуговуванням та оновленням/списанням активів;
- будь-якої організації, яка має, чи планує придбати або інвестувати у значний комплекс активів, або організації, в якій ефективне надання продукту/послуги (або виконання будь-якої іншої бізнес-цілі) безпосередньо залежить від продуктивності активів і управління ними;

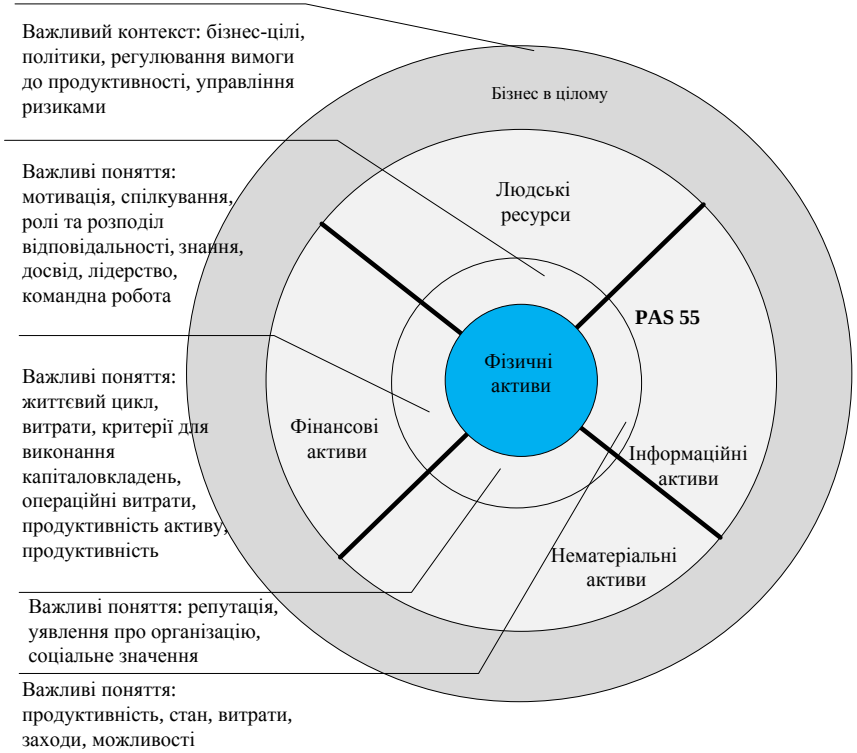


Рис. 4.10. Сфера застосування PAS 55

Сфера застосування PAS 55 в основному охоплює управління фізичними активами. Управління фізичними активами нерозривно пов'язане з іншими категоріями активів. Проте в межах цього PAS інші категорії активів розглядаються лише в тих випадках, коли вони мають безпосередній вплив на процес оптимізації управління фізичними активами. Ці критично важливі взаємозалежності представлені на рис. 4.10, який демонструє сферу застосування PAS 55 у взаємозв'язку з іншими категоріями активів.

Створення та впровадження системи управління активами є необхідністю для забезпечення безпечної та безперервної роботи підприємства.

Стандарт PAS 55 визначає тему управління активами протягом усього життєвого циклу, зокрема, активами, що грають ключову роль у діяльності організації. Таким чином, система управління

Процес менеджменту ризиків ІБ може бути застосований до всієї організації, до будь-якої окремої частини організації (наприклад, підрозділу, фізичного розташування, сервісу), до будь-якої ІС, існуючим, запланованим або наявним аспектам управління (наприклад, планування безперервності бізнесу).

Мета ОР полягає у визначенні характеристик ризиків корпоративної ІС і її ресурсів. В результаті ОР стає можливим вибрати засоби, що забезпечують бажаний рівень ІБ компанії. При ОР враховуються: цінність ресурсів, значимість загроз і уразливостей, ефективність існуючих і планованих засобів захисту. Самі показники ресурсів, значущості загроз і уразливостей, ефективність засобів захисту можуть бути визначені як кількісними (КЛ) методами, наприклад, при визначенні вартісних характеристик, так і якісними (ЯК), наприклад враховують штатні або надзвичайно небезпечні нештатні впливу зовнішнього середовища.

Для представлення повноти процесу ризик-менеджменту, у цьому розділі представлено дослідження існуючих нормативних та інструментальних засобів, методів АОР, а також детально описаний цей процес у відповідності з вимогами міжнародних стандартів.

3.1. Міжнародні стандарти оцінювання інформаційних ризиків

Для визначення типів вхідних, внутрішніх і вихідних параметрів, які використовуються для аналізу та оцінювання ризику (АОР), здійснимо дослідження відповідної сучасної нормативної бази.

Стандарт NIST 800-30

Стандарт NIST 800-30 [1] (Risk Management Guide for Information Technology Systems, розробник – NIST, США) охоплює дев'ять первинних кроків:

- характеристика системи;
- ідентифікація загроз (табл. 3.1) [1];
- ідентифікація уразливостей (табл. 3.2) [1];
- аналіз управління;
- визначення ймовірності;
- аналіз впливу;
- визначення ризику;

– рекомендації з управління;
– документування результатів.

Таблиця 3.1. Приклад ідентифікації загроз

Джерела загроз	Причина	Дія загрози
Хакер, крекер	Виклик, Его, Бунт	Хакінг, соціоінжиніринг, вторгнення і зломи, несанкціонований доступ (НСД) в ІС.
Кіберзлочинець	Руйнування інформації, інформаційне розкриття, несанкціонована модифікація даних (НМД)	Комп'ютерний злочин (кіберпереслідування), шахрайські дії, інформаційний підкуп, spoofing, вторгнення в ІС.

У процесі аналізу ризику проводиться збір інформації, ідентифікація загроз (визначення джерела, причини і дії загрози). Для оцінки використовуються такі рівні ймовірності:
– високий «В»;
– середній «С»;
– низький «Н».

Таблиця 3.2. Приклад ідентифікації пари уразливість-загроза

Уразливість	Джерело загрози	Дія загрози
ID звільнених службовців не видалені з ІС	Звільнені службовці	Проникнення в ІС на основі особистих даних
Брандмауер компанії дозволяє вхідні з'єднання telnet і на сервері XYZ включений ID гостя	Несанкціоновані користувачі (наприклад, хакери, звільнені службовці)	Використання telnet для доступу до сервера XYZ і читання системних файлів за ID гостя

При аналізі впливу визначаються події, пов'язані з втратою К, Ц і Д. Величина впливу визначається за шкалою:
– висока (В);
– середня (С);
– низька (Н).

Для визначення ризику використовується матриця РР: «В»; «С»; «Н» (табл. 3.3) [1].

BSI-Standard 100-3

BSI-Standard 100-3 [2] (Risk Analysis based on IT-Grundschutz – аналіз ризиків на основі IT-Grundschutz, розроблена Federal Office

управлінні ризиками, а також вимогах і цілях акціонерів і всіх зацікавлених сторін.

Ефективне управління активами протягом життєвого циклу вимагає дисциплінованого підходу, який дозволяє організації підвищити продуктивність активів, а також домогтися виконання стратегічних цілей. Передусім мається на увазі грамотне придбання або створення необхідних активів, з наступним визначенням оптимальних стратегій управління та обслуговування, а також вибору найкращих варіантів їх оновлення, списання та/або ліквідації [7].

Для отримання переваг PAS 55 пропонує ряд ключових принципів і визначень для розробки та впровадження системи управління активами (рис. 4.9).

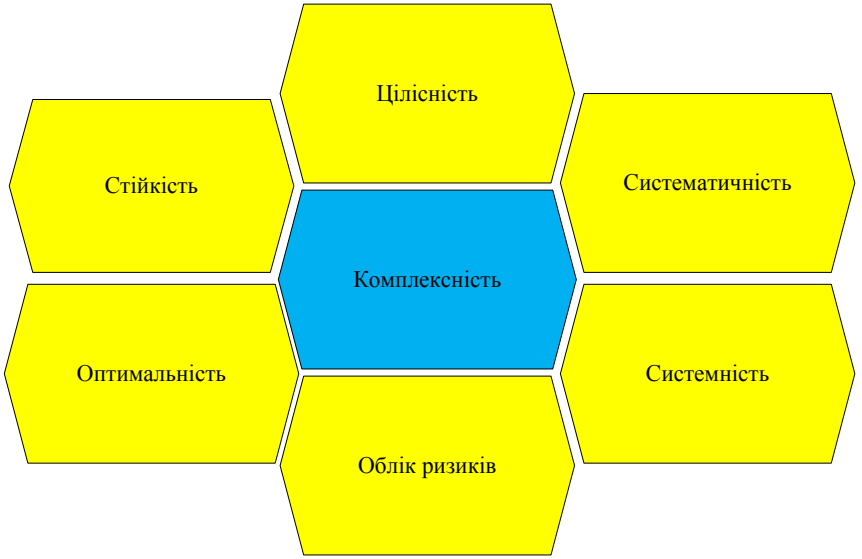


Рис. 4.9. Ключові принципи та визначення в управлінні активами

Фізичні активи (рис. 4.10) представляють лише одну з п'яти великих категорій активів, які вимагають комплексного управління для виконання стратегічного плану організації. До інших категорій належать людські активи, інформаційні активи, фінансові активи та нематеріальні активи (репутація, інтелектуальна власність, престиж фірми та ін.) [8].

Було зроблено висновок, що до елементів системи управління активами слід віднести [5]:

- політики;
- плани;
- процеси;
- інформаційні системи;
- контекст організації;
- лідерство;
- планування;
- засоби підтримки;
- виконання планів управління активами;
- оцінка результатів;
- покращення;
- та їх структурні елементи нижчих рівнів.

Як було зазначено вище, в основу стандарту ISO 55000 було покладено стандарт PAS-55, що був розроблений на замовлення Британського Інституту Стандартів (British Standards Institution) спільно з фахівцями організацій – світових лідерів в галузі управління активами, що використовують сучасні системи управління корпоративними активами як важливу складову успіху в бізнесі.

По суті даний стандарт містить специфікацію вимог (PAS 55-1 – перша частина) та рекомендацій (PAS 55-2 – друга частина) з організації управління фізичними активами.

Основне практичне застосування стандарту PAS-55 полягає насамперед у проведенні аудиту системи управління активами організації на відповідність вимогам, викладеним у першій частині стандарту (PAS 55-1), а також подальша робота й дотримання рекомендацій, викладених у другій частині (PAS 55-2) з удосконалення існуючої системи управління активами [7].

У стандарті PAS 55 дається таке визначення термінів:

Управління активами – систематична діяльність організації за оптимальним управлінням активами і системами активів, їх сукупною продуктивністю, ризиками і витратами протягом усього життєвого циклу з метою виконання стратегічного плану організації;

«*Стратегічний план організації*» – це загальний довгостроковий план розвитку та діяльності організації, який ґрунтується на її місії, цінностях, правилах ведення бізнесу, політиках в області

for Information Security – BSI, Німеччина) ґрунтується на процесі АОР ІТ-безпеки, запропонованого в BSI-Standard 100-3, включає сім етапів.

Таблиця 3.3. Матриця РР

Ймовірність загрози	**Вплив**		
	Н (10)	***С (50)***	***В (100)***
В (1,0)	**Н** 10 × 1,0 = 10	**С** 50 × 1,0 = 50	**В** 100 × 1,0 = 100
С (0,5)	**Н** 10 × 0,5 = 5	**С** 50 × 0,5 = 25	**С** 100 × 0,5 = 50
Н (0,1)	**Н** 10 × 0,1 = 1	**Н** 50 × 0,1 = 5	**Н** 100 × 0,1 = 10

Етап 1 – Попередня підготовка. На цьому етапі визначається область ІБ, вимоги до неї (нормальні, високі і дуже високі), які розглядаються з точки зору забезпечення К, Ц і Д.

Етап 2 – Підготовка опису загрози. За допомогою запропонованого в методиці списку загроз здійснюється їх аналіз для конкретного підприємства. Ідентифікуються модулі та цільові об'єкти (ЦО) захисту, які заносяться в таблицю (табл. 3.4) [2]. Кожен модуль ЗІ пов'язаний зі списком загроз, а номер і їх назва відповідає конкретному ЦО. Результатом проходження етапу є список загроз конкретного об'єкта (табл. 3.5) [2]. Далі, в узагальненій таблиці загрози упорядковуються відповідно до кожного ЦО.

Таблиця 3.4. Приклад ідентифікації

№	**Назва модуля**	**ЦО**
В 2.4	Серверна кімната	Каб. М. 723
В 2.6	Виробнича кімната	Каб. М. 811
В 3.101	Сервер	S3
В 3.207	Головний клієнт	C4
В 3.301	Шлюз безпеки (Firewall)	N3

Етап 3 – Визначення додаткових загроз.

Таблиця 3.5. Приклад опису загрози

Сервер S3
К: нормальна; Ц: висока; Д: висока
Т 1.2 Відмова ІТ-системи, Т 3.2 Ненавмисне знищення активу, Т 4.1 Перебій в живлені, Т 5.57 Мережеве сканування, Т 5.85 Втрата Ц інформації т.ін.

Етап 4 – Оцінка загрози (ОЗ). Тут проводиться тематичне опитування фахівців на основі базових запитів. Результати фіксуються

в таблиці із зазначенням Y (якщо заходи ІБ (здійснені або передбачені) забезпечують належний захист від відповідної загрози або, що загроза не важлива для поточного аналізу ступеня ризику) або N (якщо заходи ІБ (здійснені або передбачені) не забезпечують належний захист від відповідної загрози) для кожної окремої загрози (табл. 3.6)) [2].

Таблиця 3.6. Приклад ОЗ

Сервер S3	**ОЗ**
К: нормальна; Ц: висока; Д: висока	
Т 1.2 Відмова ІТ системи	N
Заходи ІБ для сервера S3 не запобігають реалізації загрози. ІТ – заходи за Каталогом Grundschutz не відповідають	
Т 5.85 Втрата Ц інформації	N
Інформація клієнта про замовлення не повинна піддаватися несанкціонованій модифікації (НСМ).	

Етап 5 – Обробка ризиків. Тут використовується шкала: «А» – зниження ризику за допомогою додаткових заходів; «В» – запобігання ризику за допомогою реструктурування; «С» – прийняття ризику; «D» – передача ризику; (табл. 3.7) [2].

Етап 6 – Консолідація концепції ІБ.

Етап 7 – Зворотній зв'язок [2].

Таблиця 3.7. Приклад таблиці обробки ризику

Сервер S3	
К: нормальна; Ц: висока; Д: висока	
Т 1.2	Відмова ІТ-системи
«А» S 6. U1	Додатковий ІТ-захід з ІБ: Здійснення повної заміни системи для спілкування з клієнтом. Реалізується повна заміна системи для зв'язку з клієнтами. Резервна система розташовується в приміщенні Е.3 з можливістю використання в будь-який момент часу, (не> 30 хв. затримки виробництва)).

Стандарт РС БР ІББС-2.2-2009

Стандарт РС БР ІББС-2.2-2009 (Рекомендації в галузі стандартизації Банку Росії, забезпечення ІБ організацій банківської системи, Російська Федерація) АОР порушення ІБ використовується для типів інформаційних активів (ІА), що входять в заздалегідь задану область оцінки. На початковому етапі визначаються:

систем дозволяє скоротити зусилля і витрати, пов'язані з розробкою і підтримкою системи управління активами. Це так само покращує інтеграцію різних функцій і координацію діяльності структурних підрозділів організації [6].

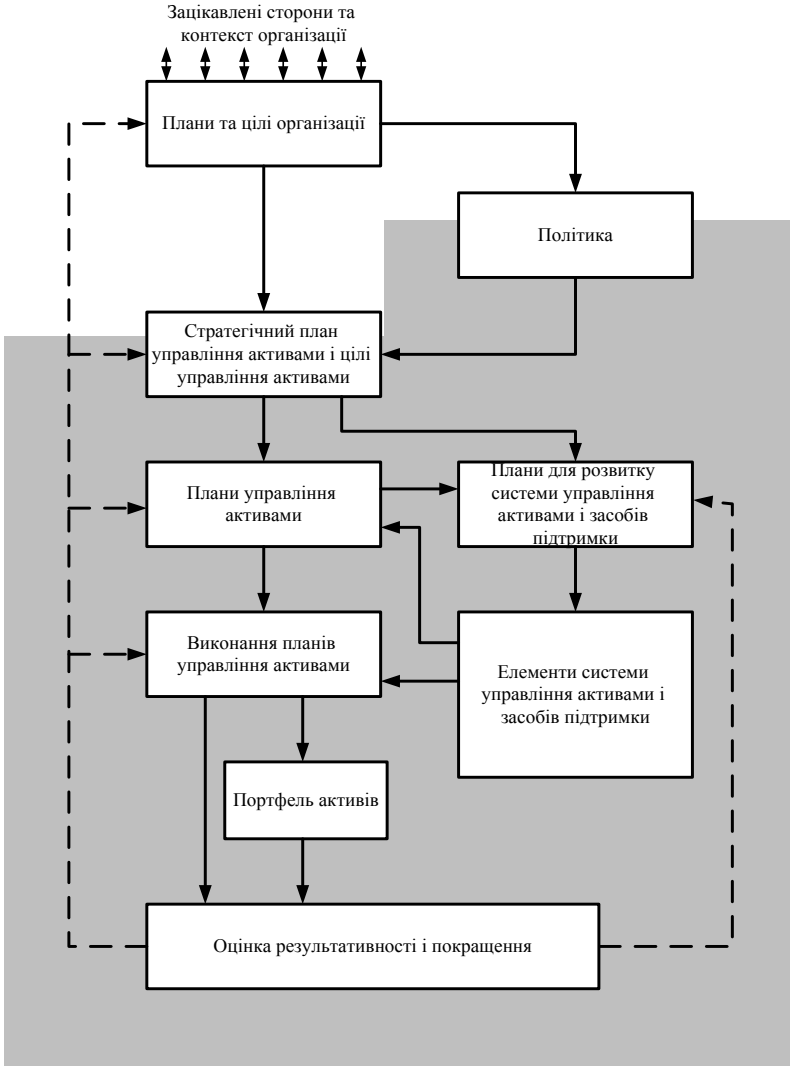


Рис. 4.8. Система управління активами згідно FDIS ISO 55000

фізичним об'єктом, таким як, наприклад, рейки, поїзди, транспортні засоби, так і нематеріальним, наприклад, репутацією компанії. Будь-який актив створює цінність для компанії, тому ним необхідно ефективно управляти для отримання найбільших вигід.

Основна перевага застосування даного стандарту – створення цінності за допомогою активів, і однією з переваг є те, що вже на ранній стадії використання можна швидко отримати багато виграшів. Ряд з них відноситься до більш докладного вивчення характеристик активів. Підхід може допомогти покращити взаємодію зі сторонами, зацікавленими в результатах діяльності компанії. Цінність не обов'язково означає дохід із грошової статті. Найчастіше обговорення цінності активу виходить за межі самої компанії або організації [6].

Підхід ISO, який включив в стандарт нематеріальні активи, відкриє нові можливості використання стандарту в тих сферах, де раніше організації і компанії не могли ним скористатися.

Отже можемо сказати, що згідно FDIS ISO 55000, система управління активами – це сукупність взаємопов'язаних або взаємодіючих елементів організації, що використовуються для розробки політики управління активами, цілей управління активами і процесів для досягнення цих цілей. Елементи системи включають організаційну структуру, права та обов'язки, планування, виконання заходів, і так далі. Таким чином, по-перше, політики, цілі та процеси на перший погляд до елементів системи не відносяться, по-друге, приблизний перелік елементів є відкритим.

Цю систему зображено на рис. 4.8, де межі системи управління активами позначені сірим кольором.

Елементи системи повинні розглядатися як інтегровані інструменти для забезпечення виконання заходів з управління активами. Процес створення системи управління активами вимагає досконального розуміння кожного її елемента, а також вимагає розуміння політик, що зв'язують ці елементи, планів і процедур.

З поняттям «елемент» тісно пов'язаний «інтегрований підхід», який визначений в стандарті FDIS ISO 55000. Використання інтегрованого підходу до системи управління активами дозволяє їй формуватися на основі елементів діючих систем управління, таких, як управління якістю, екологічний менеджмент, охорона праці та безпека, управління ризиками та ін. Формування на основі наявних

– повний перелік типів ІА, що входять в область оцінки (на основі результатів їх класифікації);

– повний перелік типів об'єктів середовища, відповідних кожному з типів ІА області оцінки;

– модель загроз ІБ, заснованої на всіх виділених типах об'єктів середовища всіх рівнів ієрархії інформаційної інфраструктури. Процес ОР порушення ІБ здійснюється на підставі ЯК оцінок ймовірності реалізації загрози (в оригіналі СМР – ступінь можливості реалізації загроз ІБ) і потенційного збитку від її реалізації (в оригіналі СТН – ступінь тяжкості наслідків від втрати властивостей ІБ для розглянутих типів ІА). Оцінка визначається на основі експертних суджень фахівців служби ІБ із залученням професіоналів в області ІТ. Для проведення ОР порушення ІБ виконується 6 процедур:

1. Визначення переліку типів ІА, для яких виконується оцінювання (тобто області ОР). Для кожного типу ІА слід визначити, які для нього властивості ІБ (К, Ц, Д і, якщо необхідно, то й інше) повинні бути забезпечені;

2. Визначення переліку типів об'єктів середовища (поділяються за рівнями інформаційної інфраструктури) відповідних кожному з типів ІА;

3. Визначення переліку актуальних джерел загроз (формується на основі моделі загроз компанії) для кожного із зазначених типів;

4. Визначення СМР загроз щодо типів об'єктів середовища. На основі п'ятиступеневої ЯК шкали («не реалізовується» (НР), «мінімальна» (МН), «середня» (С), «висока» (В), «критична» (КР)) проводиться аналіз можливості втрати властивостей ІБ для кожного з типів ІА в результаті впливу загроз. Основними чинниками для оцінки СМР загроз ІБ є:

– інформація від відповідних моделей загроз (дані про розташування джерела загрози, його мотивації і припущення про кваліфікацію (ресурси) джерела), статистичні дані про частоту реалізації загрози її джерела в минулому, інформація про способи реалізації загроз і складності їх виявлення, а також дані про наявність у розглянутих типів об'єктів середовища організаційних, технічних та інших апріорних захисних заходів;

5. Визначення СТН для типів ІА на основі аналізу наслідків втрати кожного із значущих властивостей ІБ для кожного з типів ІА в результаті впливу на відповідні їм типи об'єктів середовища виділених джерел загроз. Використовується чотирьохступенева ЯК шкала («МН», «С», «В», «КР»).

Основними чинниками для оцінювання є:

– ступінь впливу на безперервність і репутацію діяльності компанії;

– обсяг фінансових (матеріальних) втрат і витрат на відновлення властивостей ІБ ІА (ліквідації наслідків порушення ІБ – фінансових, матеріальних, тимчасових і людських ресурсів);

– ступінь порушення законодавчих вимог (договірних зобов'язань компанії), а також вимог регулюючих і контролюючих органів в області ІБ;

– обсяг інформації, яка зберігається, передається, обробляється і знищується, що відповідає розглянутому типу об'єкта середовища;

– дані про наявність у розглянутих типах об'єктів середовища організаційних, технічних та інших захисних заходів, які знижують тяжкість наслідків (апостеріорних);

6. Оцінювання ризиків порушення ІБ проводиться на підставі зіставлення СМР загроз і СТН порушення ІБ внаслідок реалізації відповідних загроз. Оцінювання проводиться для всіх значущих властивостей ІБ виділених типів ІА, всіх відповідних їм комбінацій типів об'єктів середовища і джерел загроз, які на них впливають. Використовується така ЯК шкала ризиків: допустимий (Д), недопустимий (НД). Для зіставлення СМР загроз і СТН заповнюється таблиця Д і ДП ризиків порушення ІБ (табл. 3.8) [3].

Таблиця 3.8. Д і НД ризики

СМР загроз ІБ	СТН порушення ІБ			
	МН	**С**	**В**	**КР**
НР	Д	Д	Д	Д
МН	Д	Д	Д	НД
С	Д	Д	НД	НД
В	Д	НД	НД	НД
КР	НД	НД	НД	НД

Дослідження стандартів у сфері управління активами підприємства

На сьогодні у світі розроблено багато стандартів, що допомагають забезпечити управління активами підприємства, зокрема забезпечити їх ідентифікацію та оцінку.

В даний час основним стандартом, що охоплює всі тонкості управління активами є стандарт ISO 55000 – стандарт з управління активами та різними послугами (навчання, впровадження, оцінка та стратегічне планування) – майже одноголосно затверджений для переходу в статус Міжнародного Стандарту (FDIS) [5].

У 2004 році Інститут Великобританії з управління активами, спільно з Британською Інститутом Стандартів, розробили PAS 55 – першу загальнодоступну специфікацію для оптимізованого управління матеріальними активами. Вона виявилася дуже успішною й отримала широке поширення в комунальній, транспортній, гірничодобувній, переробній та виробничій промисловостях. На теперішній час Міжнародна організація зі стандартизації (ISO) прийняла PAS 55 як основу для розвитку нової серії міжнародних стандартів ISO 55000 [5].

До складу серії ISO 55000 увійшли стандарти [5]:

– ISO 55000 представляє огляд змісту системи управління активами, умови стандарту, а також використовувані визначення.

– ISO 55001 є специфікацію вимог для ефективної інтегрованої системи управління активами.

Варто зазначити, що 55001 визначає вимоги для системи менеджменту таким же чином, як ISO 9001 визначає СМЯ, а ISO 14001 відноситься до системи менеджменту станом навколишнього середовища. Тому ISO 55001 не є специфікацією для системи обліку та організації матеріальних цінностей, що називається EAM-системою. Однак, EAM-системи визнані найбільш підходящим інструментом для створення надійної системи управління виробничими активами підприємства [6]. ISO 55002 являє посібник з впровадження системи.

У новому стандарті було визначено актив (asset) як об'єкт, одиницю або компонент, який має потенційну або реальну цінність для організації. Таке широке визначення було дано спеціально. Таким чином підкреслюється те, що актив може бути як матеріальним і

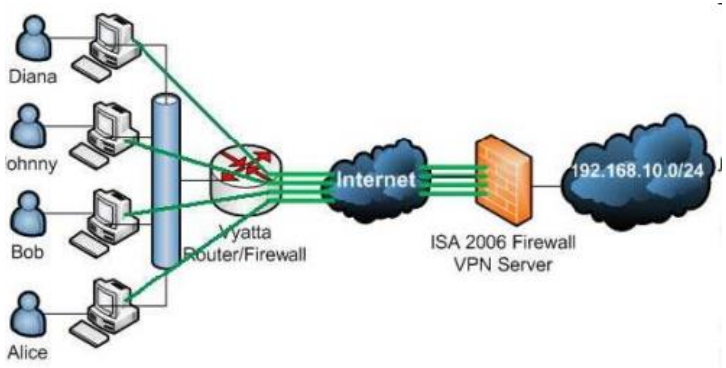


Рис. 4.6. Коротка схема розміщення активів (на прикладі матеріальних активів – Комп'ютерна та офісна техніка)

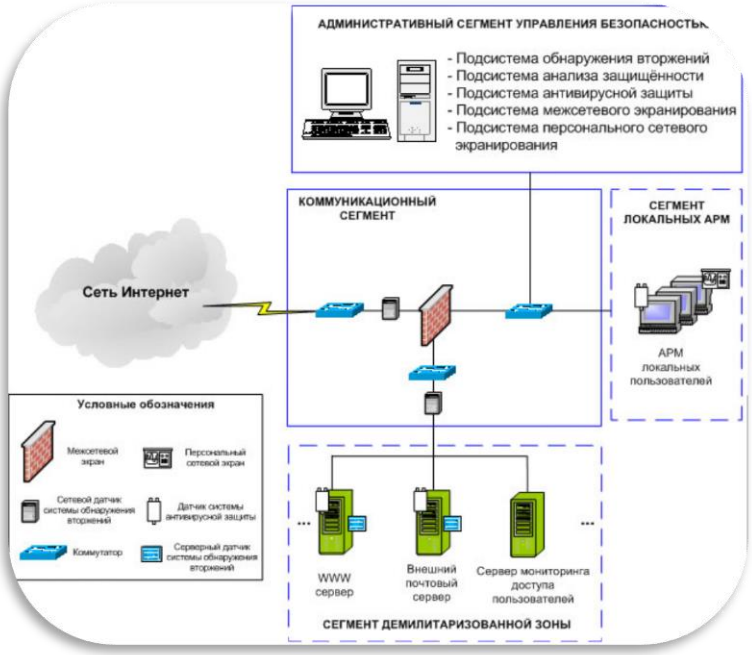


Рис. 4.7. Коротка схема розміщення активів (на прикладі матеріальних активів - Мережі та комунікації)

Ризики порушення ІБ можуть бути оцінені в КЛ (грошовій) формі на підставі оцінок СМР загроз ІБ (наприклад, в%) і СТН (наприклад, в грошовому вигляді від величини капіталу компанії (ВКК)). Кількісні оцінки також здійснюються експертними методами.

При необхідності можуть використовуватися шкали (табл. 3.9) [3] відповідності ЯК і КЛ оцінок СМР загроз і СТН.

Таблиця 3.9. Шкали відповідності

СМР загрози		СТН порушення ІБ	
($М_{як}$)	($М_{кл}$), %	($М_{як}$)	($М_{кл}$), %
НР	0	МН	[0; 0,5[
МН	]0; 20[	СР	[0,5; 1,5[
С	[20; 50[	ВС	[1,5; 3,0[
В	[50; 100[	КР	[3,0; 100] (від ВВК)
КР	100		

Кількісне ОР порушення ІБ є добутком оцінок СМР загроз і СТН для кожного із значущих властивостей ІБ виділених типів ІА і всіх відповідних їм комбінацій об'єктів середовища та джерел загроз, які на них впливають. Сумарна ОР компанії обчислюється як сума КЛ оцінок за окремими ризиками порушення ІБ. Також в методиці є переліки рекомендованих класів і джерел загроз ІБ [3].

Стандарт ISO/IEC 27005

Стандарт ISO/IEC 27005 [4, 5] (Information technology – Security techniques – Information security risk management (Інформаційна технологія – Методи захисту – Менеджмент ризиків ІБ) є технічним переглядом стандартів, скасуванням і заміною ISO/IEC TR 13335-3: 1998 та ISO/IEC TR 13335-4: 2000, Швейцарія) надає рекомендації для менеджменту ризиками ІБ організації, особливо підтримуючи вимоги «Системи менеджменту інформаційної безпеки» (ISMS) згідно ISO/IEC 27001. Процес менеджменту реалізується за шість етапів [6, 7].

Етап 1 – Створення контексту. Здійснюється загальний аналіз всієї інформації про організацію, яка відноситься до створення контексту, а також проводиться встановлення основних критеріїв, необхідних для управління ризиками ІБ та визначення для нього області застосування і меж здійснення.

Етап 2 – ОР. Тут здійснюється ідентифікація (активів, загроз, існуючих вимог, уразливостей і наслідків), оцінювання та опис (ЯК, КЛ або їх комбінація), розташування за пріоритетами ризиків, які відносяться до організації. Якісна оцінка використовує шкалу кваліфікації атрибутів, щоб описати величину потенційних наслідків (наприклад: низькі, середні або високі) та ймовірність, реалізації цих наслідків. Кількісна оцінка використовує масштаб з числовими значеннями як для наслідків, так і ймовірності. Така оцінка в більшості випадків використовує статистику інцидентів. Результатами проходження даного етапу будуть оцінки наслідків, ймовірності інциденту і рівень ризику (РР).

Етап 3 – Обробка ризиків. Включає загальний опис обробки, а також зниження, збереження, запобігання і перенесення ризику.

Етап 4 – Прийняття ризику.

Етап 5 – Комунікації ризику.

Етап 6 – Моніторинг та перегляд ризику ІБ.

Тут здійснюється моніторинг та перегляд чинників ризику, а також поліпшення його менеджменту. У стандарті присутні рекомендації та приклади:

– визначення області застосування і меж процесу менеджменту ризиків (Додаток А стандарту);

– ідентифікації та визначення цінності активів, вартості впливу (Додаток В стандарту);

– типових загроз (Додаток С стандарту, табл. 3.10 [5], де мітки мають таке значення: D – навмисний (навмисні акції, націлені на ІА), А – випадковий (ненавмисні дії людини на ІА) і Е – екологічний (інциденти, що не засновані на діях людини));

Таблиця 3.10. Приклади типових загроз

Тип	Загрози	Мітки
НСД	Несанкціоноване використання обладнання	D
	Шахрайське копіювання ПЗ	D
	Використання підроблених або скопійованих ПЗ	A, D
	Спотворення даних	D
	Незаконна обробка даних	D

– уразливостей та методів їх оцінювання (Додаток D стандарту, див. приклад уразливостей для апаратних засобів в табл. 3.11 [5]);

Класифікація інформації може відображатися у наступних кроках:

1. Класифікація активів;
2. Маркування активів;
3. Регулярне оновлення реєстру активів.

Види активів:

а) інформаційні ресурси (бази і файли даних, контракти й угоди, системна та інша документація, інформація науково-дослідного характеру, навчальні матеріали тощо);

б) програмне забезпечення;

в) матеріальні активи (комп'ютерне обладнання (див. рис. 4.5 та 4.6), засоби телекомунікацій (див. рис. 4.7) та ін.);

г) сервіси (послуги телекомунікацій, системи забезпечення життєдіяльності та ін.);

д) співробітники компанії, їх кваліфікація і досвід;

е) нематеріальні ресурси (репутація та імідж компанії).

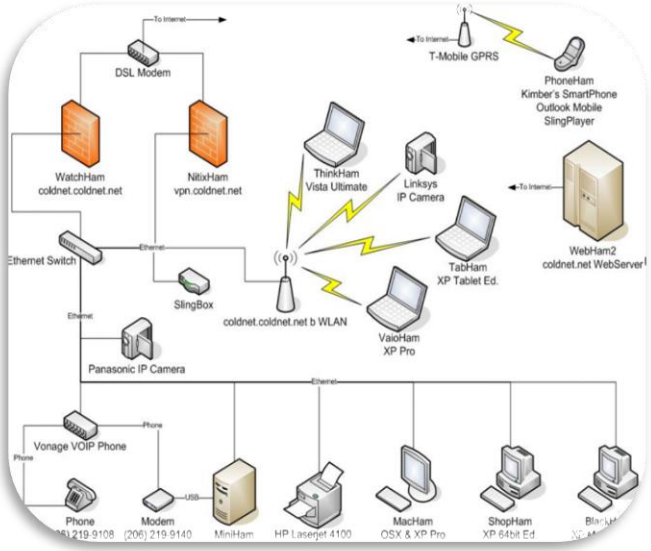


Рис. 4.5. Детальна схема розміщення активів (на прикладі матеріальних активів – Комп'ютерна та офісна техніка)

д) утилізація критичних носіїв повинна реєструватися для пред'явлення як свідчення під час аудиту.

При накопиченні носіїв для утилізації слід мати на увазі ефект критичної маси, який проявляється в тому, що великий масив некритичною інформації сам може стати критичним.

3) Фізичні носії під час передавання. Носії, що містять інформацію, має бути захищено від несанкціонованого доступу, зловживання чи руйнування під час транспортування.

Для захисту носіїв інформації, що транспортуються, повинні бути прийняті до уваги наступні рекомендації:

а) повинен використовуватися надійний транспорт або кур'єри;

б) перелік авторизованих кур'єрів повинен бути погоджений з керівництвом;

в) повинні бути розроблені процедури для ідентифікації кур'єрів;

г) упаковка повинна забезпечувати захист вмісту від будь-яких фізичних ушкоджень, які можуть виникнути в ході транспортування, і відповідати вимогам виробників, наприклад, захист від будь-яких зовнішніх факторів, які можуть знизити можливість відновлення носіїв, такі як вплив тепла, вологи або електромагнітних полів;

д) повинні вестися записи, які вказують вміст носіїв, застосований захист, а також час передачі для транспортування і прийому в місці призначення.

Інформація може бути уразливою для несанкціонованого доступу, нецільового використання або пошкодження під час фізичної транспортування, наприклад, при відправці носія поштою або через кур'єра. В цьому випадку носії включають у себе і паперові документи.

У тих випадках, коли конфіденційна інформація не зашифрована, повинні передбачатися додаткові заходи фізичного захисту носія [1, 2].

Процес *встановлення відповідальність* за активи може описуватися декількома кроками:

1. Реєстр активів;
2. Призначення власників активів;
3. Правила поводження з активами;
4. Оцінка активів.

Таблиця 3.11. Приклади уразливостей і загроз

Уразливості	Загрози
Недостатнє обслуговування (дефектна інсталяція)	Прогалина в можливості ремонту ІС
Вади схем для періодичних замін	Руйнування обладнання (носіїв)
Вади ефективного контролю внесення змін конфігурації	Помилка у використанні
Сприйнятливість до перепадів живлення	Втрата джерела живлення

– підходів до ОР (Додаток Е стандарту, табл. 3.12 – 13 [5]);
– обмеження щодо зниження ризику (Додаток F стандарту).

Стандарт має реалізації в ПЗ, наприклад, Meycor KP (Knowledge Provider). В ISO/IEC 27005 запропоновано високорівневе і детальне ОР ІБ. Для останньої може використовуватися матриця зі значеннями за замовченням (див. табл. 3.12 [5]). Для кожного активу розглядаються відповідні уразливості і загрози, наприклад, якщо цінність активу – (ЦА) = 3, ймовірність виникнення (ЙВ) загрози – (ЙВЗ) = «В» і простота використання уразливості – (ПВУ) = «Н», то міра ризику – (МР) = 5.

Таблиця 3.12. Матриця оцінки МР

ЙВЗ		**Н**			**С**			**В**		
ПВУ		**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
ЦА	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	**5**	6	7
	4	4	5	6	5	6	7	6	7	8

Також запропонована матриця визначення ймовірності сценарію інциденту (ЙСІ) (див. табл. 3.13 [5], де «ДН» (дуже низька), «Н» (низька), «С» (середня), «В» (висока), «ДВ» (дуже висока)), що відповідно означає (дуже малоймовірно), (малоймовірно), (можливо), (ймовірно), (часто).

Отримане результуюче значення ризику вимірюється за шкалою від 0 до 8 (наприклад, «Н» (0-2); «С» (3-5); «В» (6-8)) і може бути оцінене відповідно до критеріїв прийняття ризику. У додатку стан-

дарту розглянуто приклад ранжирування загроз за допомогою МР (див. табл. 3.14 [5]).

Таблиця 3.13. Матриця визначення ЙСІ

	ЙСІ	ДН	Н	С	В	ДВ
Вплив на бізнес	ОН	0	1	2	3	4
	Н	1	2	3	4	5
	С	2	3	4	5	**6**
	В	3	4	5	**6**	**7**
	ОВ	4	5	**6**	**7**	**8**

Матриця може використовуватися для зв'язку чинників наслідків ЦА з ЙВЗ (беручи до уваги аспекти уразливості). Спочатку за певною шкалою (наприклад, 1 ÷ 5) проводиться оцінка ЦА для кожного активу, який знаходиться під загрозою (колонка (b)).

Далі, наприклад, за тією ж шкалою оцінюється ЙВЗ, для кожної загрози (колонка (c)) і за отриманими результатами обчислюється міра ризику (колонка (d)) шляхом множення d = b × c. Далі проводиться ранжування загроз (колонка (e)) в порядку відповідної міри ризику (в табл. 3.14 [5] 1 – найнижчий наслідок і найнижча ЙВЗ. У колонці (a) відображені ідентифікатори загроз).

Таблиця 3.14. Приклад ранжування загроз

(a)	(b)	(c)	(d)	(e)
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5
E	4	1	4	4
F	2	4	8	3

Розглянемо приклад, в якому особлива увага приділяється наслідкам інцидентів ІБ та визначенню того, яким системам слід віддавати перевагу.

Це виконується шляхом оцінювання двох значень для кожного активу і загрози, комбінація яких буде визначати бали ($Б_{ij}$), де i і j – відповідно номер активу і загрози.

Підсумовування всіх балів активів дає можливість визначити МР. Спочатку кожному активу присвоюється ЦА для кожного випадку виникнення відповідної загрози. Далі визначається показник

г) в тому випадку, якщо дані є конфіденційними або важлива їх цілісність, повинні застосовуватися криптографічні методи для захисту даних на знімних носіях,

д) для зниження ризику, пов'язаного з погіршенням властивостей носія від часу, в тому випадку, коли дані ще необхідні, вони повинні бути переписані на новий носій до того, як стануть нечитабельним,

е) кілька копій важливих даних повинні зберігатися на окремих носіях для зниження ризику одночасної втрати або пошкодження даних,

ж) повинна передбачатися реєстрація знімних носіїв для обмеження можливості втрати даних,

з) носії, що знімаються, повинні застосовуватися тільки в тому випадку, якщо це виправдано потребами бізнесу,

и) там, де є необхідність застосування носіїв, що знімаються, перенесення інформації на них повинно контролюватися.

Процедури і рівні авторизації повинні бути задокументовані.

2) Вилучення носіїв. Коли носії більше не потрібні, їх треба безпечно вилучати із застосуванням офіційно оформлених процедур.

Повинні бути встановлені формальні процедури для надійної утилізації носіїв з метою мінімізації ризику витоку конфіденційної інформації щодо осіб, яким вона не призначена. Процедури для надійної утилізації носіїв, які містять конфіденційну інформацію, повинні відповідати ступеню критичності цієї інформації. При цьому повинно бути враховано наступне:

а) носії з конфіденційною інформацією повинні зберігатися і утилізуватися надійним способом, наприклад, спалюванням або подрібненням, чи очищатися від даних для застосування іншою програмою в організації;

б) процедури повинні бути введені в дію, щоб визначати ті елементи, які можуть вимагати утилізації;

в) може бути простіше організувати для всіх носіїв збір і надійну утилізацію, ніж намагатися відокремити критичні;

г) багато організацій пропонують послуги збору та утилізації носіїв але необхідно уважно вибирати відповідного зовнішнього виконавця, який застосовує відповідні засоби і має досвід;

Таблиця 4.2. Приклад оцінки та класифікація активів

Назва рівня	Визначення в грошових одиницях	Визначення з точки зору впливу на репутацію компанії
Низький рівень	Незначний збиток до 10 тис. грн.	Незначний вплив на репутацію компанії
Середній рівень	Помітний збиток від 10 тис. до 100 тис. грн.	Істотний вплив на репутацію компанії або обмеження її інтересів
Високий рівень	Значний збиток від 100 тис. грн.	Шкода репутації компанії і її інтересам, яка може становити загрозу для продовження діяльності компанії аж до повного банкрутства

Приклад: Персональний комп'ютер

- За видом активу - матеріальний актив - МА.
- За вартістю активу - низький рівень (2900 грн.) - Н.
- За власником активу - юрист, юр. відділ - ЮЮ.
- Ідентифікація активу - МА_036_Н_ЮЮ.

Поводження з носіями.

Ціль: Запобігти несанкціонованому розголошенню, модифікації, вилученню або знищенню інформації, яка зберігається на носіях.

1) Управління змінними носіями. Має бути впроваджено процедури управління змінними носіями відповідно до схеми класифікації, запровадженої в організації.

Для управління знімними носіями повинні бути враховані такі рекомендації:

а) вміст, в якому відпала необхідність, на будь-яких багаторазово використовуваних носіях, які можуть бути винесені з організації, повинен бути видалений без можливості відновлення,

б) там, де це необхідно і доцільно, має вимагатися дозвіл для носіїв, які виносяться з території організації, і записи про винесення повинні зберігатися для пред'явлення як свідчення під час аудиту,

в) усі носії повинні зберігатися в безпечному, захищеному місці відповідно до вимог виробника,

ймовірності ризику (ПЙР). Він оцінюється на підставі з комбінації ЙВЗ і ПВУ (див. табл. 3.15 [5]).

Таблиця 3.15. Приклад оцінки

ЙВЗ	**Н**			**С**			**В**		
ПВУ	Н	С	В	Н	С	В	Н	С	В
ПЙР	0	**1**	2	1	2	**3**	2	3	4

На наступному кроці за перетином ліній значень ЦА і ПЙР в табл. 3.16 [5] присвоюються відповідні бали, після чого вони підраховуються для отримання підсумкових значень з кожного активу.

Таблиця 3.16. Бальник

ПЙР	**ЦА**				
0	0	1	2	3	4
1	1	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	**6**	7
4	4	5	6	7	8

Далі припустимо, що система С має три активи $А_1$, $А_2$, $А_3$ і існують дві загрози $З_1$, $З_2$ цій системі. Нехай $ЦА_1 = 3$, $ЦА_2 = 2$ та $ЦА_3 = 4$. Якщо для $А_1$ і $З_1$ $ЙВЗ_{11}$ = «Н» та $ПВУ_{11}$ = «С», то значення $ПЙР_{11} = 1$ (див. табл. 3.15 [5]).

Бали для $А_1$ і $З_1$ можуть бути визначені з табл. 3.16 [5] на перетині ліній $ЦА_1 = 3$ та $ПЙР_{11} = 1$, тобто $Б_{11} = 4$. Аналогічним чином, нехай для $А_1$ і $З_2$ $ЙВЗ_{12}$ = «С», а $ПВЗ_{12}$ = «В», то $ПЙР_{12} = 3$, тобто $Б_{12} = 6$. Тепер можна обчислити сумарні бали ($БІ_i$) активу щодо всіх загроз $БІ_1 = Б_{11} + Б_{12} = 10$. Обчислення підсумкових балів до всієї системи (БІС) проводиться шляхом підсумовування всіх балів за кожним активом щодо всіх загроз $БІС = БІ_1 + БІ_2 + БІ_3$ [5]. У стандартах ISO/IEC 27001 та 27002 на етапі ОР ІБ дається посилання на документ ISO/IEC TR 13335-3, який тепер представлений як ISO/IEC 27005.

Стандарт AS/NZS 4360:2004

Стандарт AS/NZS 4360: 2004 [8] (Австралія і Нова Зеландія) надає рекомендації з АОР, які проводиться за 7 етапів.

1. Визначення контексту оцінки ступеня ризику.

2. Ідентифікація ризику, що ґрунтується на ініціалізації табл. 3.17 [8].

Таблиця 3.17. Ідентифікація та аналіз ризику

Посилання ризику	Ризик Що може відбутись?	Джерело Як може це відбуватись?	Вплив від реалізації ризику	Поточні стратегії управління та їх ефективність (А) – адекватні; (М) – помірні; (І) – недостатні.	РР			Прийнятність
					Ймовірність	Наслідок	Поточний РР	

3. Аналіз ступеня ризику. Визначаються наслідки (L), ймовірність (Р) і РР за допомогою матриці ризику (табл. 3.18 [8]).

Таблиця 3.18. Приклад матриці ризику

Де Е – Надзвичайний ризик (необхідно деталізувати потрібний план дій);
Н – Високий ризик (необхідна увага вищого керівництва);
М – Середній ризик (визначає управлінську відповідальність);
L – Низький ризик (обробляється звичайними процедурами).

					Наслідок				
				Бізнес-процес& Системи	Незначні помилки в системах або процесах, що вимагають коригувальних дій, або незначної затримки без впливу на повний графік.	Стратегічна процесуальна норма, час від часу не зустрічається або послуги, в повному обсязі задовольняють потребам.	Одне або більше ключових вимог не будуть виконані.	Стратегії не сумісні з порядком денним уряду. Тенденції показують, що обслуговування погіршується	Критична системна відмова, поганий стратегічний план або тривале недотримання. Бізнес серйозно постраждав.
				Фінансові	1% від бюджету або <$5 тис.	2,5% від бюджету або <$50 тис.	> 5% від бюджету або <$500 тис.	> 10% від бюджету або <$5 млн.	>25% від бюджету або >$5 млн.
					Незначне	**Мале**	**Помірне**	**Велике**	**Катастрофічне**
	Ймовірність	**Статистика**			**1**	**2**	**3**	**4**	**5**
Ймовірність	> 1 при 10	Відбудеться в більшості випадків	**5**	**Майже безперечно**	**M**	**H**	**H**	**E**	**E**
	1 при 10 - 100	Ймовірно відбудеться	**4**	**Ймовірно**	**M**	**M**	**H**	**H**	**E**
	1 при 100 – 1 000	Можуть відбутися в майбутньому	**3**	**Можливо**	**L**	**M**	**M**	**H**	**E**
	1 при 1 000 – 10 000	Можуть відбутися, але сумнівно	**2**	**Навряд**	**L**	**M**	**M**	**H**	**H**
	1 при 10 000 – 100 000	Можуть відбутися при виняткових обставинах	**1**	**Рідко**	**L**	**L**	**M**	**M**	**H**

Результати, що формуються системами, що містить інформацію, яка класифікована як конфіденційна або значуща, повинні оброблятися відповідно до класифікаційної категорії.

Маркування конфіденційної інформації є ключовою вимогою для заходів з обміну інформацією. Звичайною формою маркування є наклеювання етикеток і вказівку метаданих.

3) Поводження з активами СМІБ. Має бути розроблено та впроваджено процедури поводження з активами СМІБ відповідно до схеми класифікації інформації, яку офіційно прийнято в організації.

Процедури повинні бути розроблені для звернення, обробки, зберігання та передачі інформації відповідно до категорії класифікації.

Мають бути прийняті до уваги такі чинники:

а) обмеження доступу, що забезпечують виконання вимог щодо захисту для кожної категорії класифікації;

б) ведення документованого реєстру уповноважених власників активів;

в) захист тимчасових або постійних копій інформації на рівні, відповідному захисту оригінальної інформації;

г) зберігання ІТ-активів відповідно до вказівок виробників;

д) чітке маркування всіх копій носіїв для інформування уповноваженого власника.

Схема класифікації (див. приклад в табл. 4.2), яка використовується в організації, може не збігатися з подібними схемами в інших організаціях, навіть якщо збігаються найменування категорій. До того ж, інформація, передана між організаціями, може відноситися до різних категорій класифікації залежно від ситуації в кожній організації, навіть якщо їх схеми класифікації ідентичні.

Угоди з іншими організаціями, які передбачають спільне використання інформації, повинні включати в себе процедури визначення класифікації такої інформації і інтерпретації категорій класифікації для інших організацій.

Можлива трирівнева класифікація активів:

– за видом активу;
– за вартістю активу;
– за власником активу.

інформації за однаковими необхідними заходами захисту і визначення процедур ІБ, які застосовуються до всієї інформації кожної категорії, полегшує це завдання. Такий підхід знижує потребу в оцінюванні ризиків і виборі засобів реалізації в кожному окремому випадку.

Ступінь конфіденційності або значимості інформації може змінюватися після закінчення певного періоду часу, наприклад, після її опублікування. Подібні фактори повинні прийматися до уваги, тому що віднесення до більш високої категорії може вести до застосування методів реалізації, в яких немає необхідності, що веде до додаткових витрат, або навпаки, віднесення до нижчої категорії може ставити під загрозу досягнення бізнес-цілей.

Орієнтовна схема класифікації з конфіденційності, може ґрунтуватися на наступних чотирьох рівнях:

а) розкриття не викликає шкоди;

б) розкриття створює деякі труднощі або невеликі проблеми в операційній діяльності;

в) розкриття надає істотний короткочасний ефект на операційну діяльність або досягнення тактичних цілей;

г) розкриття чинить серйозний вплив на досягнення довгострокових стратегічних цілей або піддає ризику саме існування організації.

2) Маркування інформації. Має бути розроблено та впроваджено належну множину процедур для маркування й оброблення інформації згідно зі схемою класифікації, прийнятою організацією.

Процедури для маркування інформації повинні охоплювати інформацію і пов'язані з нею активи, як у фізичній, так і в електронній формі. Маркування має відповідати схемі класифікації, встановленої в організації. Маркування повинно легко розпізнаватися. Процедури повинні містити керівні вказівки, де і як розміщується маркування з урахуванням того, яким чином здійснюється доступ до інформації або способів використання активів, що залежать від типу носія. Процедури повинні визначати ситуації, коли маркування – щоб уникнути зайвих витрат – не потрібне, наприклад, для інформації, яка не є конфіденційною. Співробітники і працюючи за контрактом повинні бути ознайомлені з процедурами маркування інформації.

4. ОР. Порівнюються оцінені РР за попередньо встановленими критеріями.

5. Обробка ризику.

6. Контроль.

7. Консультації [8].

Стандарт ISO/FDIS 31000

Стандарт ISO/FDIS 31000 [9] (Risk management – Principles and guidelines (Управління ризиками – керівні принципи), Швейцарія) описує основні принципи АОР. У ньому визначено 7 основних етапів управління ризиками:

1. Опис структури організації та її контексту;

2. Визначення політики ризик-менеджменту. Політика повинна чітко відображати цілі організації;

3. Визначення відповідальності;

4. Інтеграція в організаційні процеси;

5. Ідентифікація ресурсів;

6. Створення внутрішніх зв'язків і механізмів звітності;

7. Створення зовнішніх зв'язків і механізмів звітності організації.

Для проведення АОР встановлюються критерії ризику, які повинні відобразити цілі та ресурси організації, бути сумісними з її політикою ризик-менеджменту, визначеною на початку будь-якого процесу ризик-менеджменту і постійно переглядатись.

Далі переходять до процесу оцінювання ступеня ризику – повний процес його ідентифікації, аналізу та оцінювання.

На етапі аналізу визначаються наслідки, ймовірність та інші ознаки ризику [7, 9-11].

3.2. Сучасні методи і засоби оцінювання ризиків

За аналогією з п. 3.1 здійснимо аналіз вхідних, внутрішніх і вихідних параметрів, які використовуються для АОР в подібних методах і засобах.

Метод CRAMM

Метод CRAMM (CCTA Risk Analysis and Management Method, розробник – CCTA, Великобританія) реалізований фірмою Insight Consulting Limited в однойменному програмному продукті [12]. Відповідно до цього методу оцінювання здійснюється в три етапи. На першому – проводиться ідентифікація фізичних, програмних і інформаційних ресурсів, які містяться всередині кордонів системи.

Цінність фізичних ресурсів в CRAMM визначається вартістю їх відновлення в разі руйнування. Для даних і ПЗ вибираються критерії, які застосовуються до даної ІС, дається оцінка збитку за шкалою зі значеннями від 1 до 10. Наприклад, шкала оцінки за критерієм «Фінансові втрати, пов'язані з відновленням ресурсів» відображається через такі значення [12, 13]:

– 2 бали – менш $ 1000;
– 6 балів – від $ 1000 до $ 10 000;
– 10 балів – понад $ 100 000 тощо.

На другому етапі розглядається все, що відноситься до ідентифікації і оцінки рівнів загроз для груп ресурсів та їх уразливостей.

Програмний засіб CRAMM для кожної групи ресурсів (і кожного з 36 типів загроз) генерує список запитів, для яких після ініціалізації даних оцінювання рівнів здійснюється, наприклад, як – дуже високий, високий, середній, низький, дуже низький (для загрози), і як – високий, середній та низький (для уразливості). Загрози та уразливості об'єднуються в матриці ризику, а для створення шкал, наприклад, використовуються дані з табл. 3.19.

Таблиця 3.19. Шкали для рівнів загроз та уразливостей

Шкали	Опис	Значення
Шкала оцінки рівнів загрози (частота виникнення)	Інцидент відбувається в середньому не частіше, ніж кожні 10 років	дуже низький
	Інцидент відбувається в середньому один раз на 3 роки	низький
	Інцидент відбувається в середньому раз на рік	середній
	Інцидент відбувається в середньому раз на чотири місяці	високий
	Інцидент відбувається в середньому раз на місяць	дуже високий
Шкала оцінки рівня уразливості (ймовірність успішної реалізації загрози)	У разі виникнення інциденту ймовірність розвитку подій за найгіршим сценарієм менше 0,33	низький
	У разі виникнення інциденту ймовірність розвитку подій за найгіршим сценарієм в межах від 0,33 до 0,66	середній
	У разі виникнення інциденту ймовірність розвитку подій за найгіршим сценарієм вище 0,66	високий

відповідної інформації (наприклад, інтелектуальної власності) з боку тих, з ким припиняються трудові відносини.

Класифікація інформації.

Ціль: Забезпечити належний рівень захисту інформації відповідно до її важливості для організації.

1) Класифікація інформації. Інформація має бути класифікована в термінах правових вимог, її цінності, критичності й чутливості для неавторизованого розкриття чи модифікації.

Класифікація та пов'язані з нею методи ЗІ повинні враховувати потреби бізнесу в обміні інформацією або обмеження доступу до неї, так само як і законодавчі вимоги. Активи, що відрізняються від інформації, можуть також бути класифіковані відповідно до класифікації для інформації, яка в них зберігається, обробляється чи іншим чином перетворюється, або захищається цими активами.

Власники активів повинні бути відповідальними за їх класифікацію.

Схема класифікації повинна включати в себе угоду про класифікацію та критерії для перегляду класифікації через якийсь час. Рівень захисту в схемі повинен бути оцінений на основі аналізу конфіденційності, цілісності й можливості застосування, а також будь-яких інших вимог, пов'язаних з інформацією. Схема повинна бути узгоджена з політикою контролю доступу.

Кожному рівню має бути присвоєно найменування, яке має сенс в контексті застосування цієї класифікаційної схеми.

Схема повинна бути єдиною для всієї організації, щоб всі, хто будуть класифікувати інформацію і пов'язані з нею активи, робили це однаково, мали загальне розуміння вимог захисту і застосовували відповідні заходи захисту.

Класифікація повинна бути включена в процеси організації, бути єдиною і логічно несуперечливою в рамках організації. Результати класифікації повинні відображати цінність активів, що залежить від ступеня їхньої закритості й значущості для організації, наприклад, з точки зору конфіденційності, цілісності й доступності. Результати класифікації повинні оновлюватися відповідно до виміру цієї цінності, ступеня конфіденційності і значущості протягом всього їх життєвого циклу.

Класифікація дає тим, хто працює з інформацією, чітке розуміння, як поводитися з нею і захищати її. Формування категорій

Виконання типових задач може бути делеговане, наприклад, відповідального за зберігання, який стежить за активом на щоденній основі, але при цьому відповідальність залишається на власнику.

У складних ІС може бути корисно визначати групу активів, які спільно забезпечують певний сервіс. У цьому випадку власник цього сервісу є відповідальним за постачання цього сервісу, включаючи дії з його активами.

3) Припустиме використання активів СМІБ. Правила щодо припустимого використання інформації та активів СМІБ, пов'язаних із засобами оброблення інформації, мають бути ідентифіковані, задокументовані та впроваджені.

Співробітники і зовнішні користувачі, які використовують або мають доступ до активів організації, повинні бути ознайомлені з вимогами ІБ, що відносяться до інформації та інших активів організації, які пов'язані з інформацією, пристроями і ресурсами для обробки інформації. Вони повинні нести відповідальність за застосування ними будь-яких ресурсів обробки інформації і будь-яке подібне використання, здійснюване в зоні їх відповідальності.

4) Повернення активів СМІБ. Увесь найманий персонал та користувачі зовнішньої сторони повинні повернути всі активи СМІБ організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди.

Процес припинення трудових відносин повинен бути встановлений так, щоб включати в себе повернення всіх раніше виданих фізичних або електронних активів, що належать організації або довіреній організації.

У тих випадках, коли співробітник або зовнішній користувач купив обладнання організації або використовує своє особисте обладнання, процедури повинні бути такими, щоб гарантувати, що відповідна інформація передана в організацію і надійним способом стерта з цього обладнання.

У тих випадках, коли співробітник або зовнішній користувач володіє знаннями, цінними для поточної діяльності, такого роду інформація повинна бути документально підтверджена, передана в організацію.

У період після повідомлення до припинення трудових відносин організація повинна контролювати неавторизоване копіювання

Аналіз ризику проводиться на першому та другому етапах, після чого здійснюється його оцінювання. Під час аналізу пропонується виставити коефіцієнти для кожного ресурсу з точки зору частоти виникнення загрози та ймовірності її реалізації. Виходячи з оцінок вартості ресурсів ІС, що захищається, загроз та уразливостей, визначаються «очікувані річні втрати».

Розглянемо приклад матриці оцінки очікуваних втрат [13] (рис. 3.1, *а*), де друга колонка зліва містить значення вартості ресурсу при цьому використовується грошова шкала (рис. 3.1, *б*), верхній рядок заголовку таблиці – оцінку частоти виникнення загрози протягом року (рівня загрози), а нижній рядок заголовку – оцінку ймовірності успіху реалізації загрози (рівня уразливості).

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

а)

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

б)

Рис. 3.1. Приклад роботи систем:
а) матриця очікуваних річних втрат; б) шкала оцінки

Значення очікуваних річних втрат (Annual Loss of Expectancy) переводяться в бали, що показують РР згідно шкали, представленої на рис. 3.1, б) (в цьому прикладі розмір втрат наводиться в фунтах стерлінгах) та далі відповідно до матриці (рис. 3.2), виводиться ОР.

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 3.2. Матриця ОР

Третій етап реалізує пошук адекватних контрзаходів. Тут CRAMM генерує кілька варіантів заходів протидії, адекватних виявленим ризикам та їх рівням. ОЗ і уразливостей здійснюється на основі ОР за двома чинниками – ризик розглядається як комбінація ймовірності реалізації загрози та уразливості, а також шкоди [7, 12-14].

Метод на основі байєсовских мереж (МБМ)

Метод МБМ [15] розроблений для побудови каузальних моделей оцінки операційних ризиків. В його основі лежить теорема Байєса, цінність якої стосовно оцінки таких ризиків полягає в її здатності комбінувати дані про ймовірність подій, одержаних експертним і статистичними шляхом. Кожній пов'язаній з ризиком події (наприклад «Хакерська атака», «НСД», «НСМ» та ін.) проводиться оцінювання ймовірності її реалізації та (за ланцюжком) операційних втрат, що з нею пов'язані. Імовірність реалізації події може бути вказана у вигляді безперервної функції розподілу або у вигляді таблиці ймовірностей (дискретних ймовірностей). Приклад експертного відображення умовної ймовірності показаний в табл. 3.20 [15].

Таблиця 3.20. Формування ймовірності

	Результати - умови			
Хакерська атака	ТАК		НІ	
Зараження вірусом	Так	Ні	Так	Ні
Ймовірність результату події «Зупинка сервера» для різних умов				
Відбудеться	0,3	0,15	0,10	0,02
Не відбудеться	0,7	0,85	0,90	0,98

Процес складання реєстру активів є важливою передумовою управління ризиками (див. табл. 4.1).

Таблиця 4.1. Приклад реєстру активів

Ідентифікатор	**Найменування**	**Вид активу**	**Вартість**	**Власник**	**Місцезнаходження**
Матеріальні активи					
МА_036_Н_ЮЮ	ПК 036	МА	2900	Юрист	Юр. відділ
МА_003_С_СА	СР 003	МА	12000	Сист.Адм.	Північна 1
Інформація					
ІН_572_С_ПР	Стратегічний план розвитку	ІН	50000	Президент	ПК 020

2) Володіння активами СМІБ. Активи СМІБ, які наявні в інвентарному описі, мають «бути у власності».

Окремі особи, так само як і підрозділи, які мають затверджену відповідальність за актив протягом його життєвого циклу, можуть бути призначені власниками активу.

Процес, який гарантує своєчасне призначення власника активу, як правило, виконується. Власник повинен бути призначений, коли актив створюється або коли передається в організацію. Власник активу повинен нести відповідальність за належне управління активом протягом усього життєвого циклу активу.

Власник активу повинен:

а) гарантувати, що активи включені до реєстру;

б) гарантувати, що активи належним чином класифіковані й захищені;

в) встановити і періодично переглядати обмеження доступу та класифікацію важливих активів, беручи до уваги чинні політики контролю доступу;

г) гарантувати належні дії з активом, коли він видаляється або знищується.

Призначений власник може бути або окремою особою, або підрозділом, який має затверджену відповідальність за актив протягом усього його життєвого циклу. Призначення власником процесу не дає прав власності на актив.

Активи – ресурси, контрольовані підприємством у результаті минулих подій, використання яких, як очікується, приведе до отримання економічних вигід у майбутньому [4].

Відповідальність за активи СМІБ.

Ціль: Ідентифікувати активи СМІБ організації й визначити відповідні обов'язки щодо їх захисту.

1) Інвентаризація активів СМІБ. Інформація, активи СМІБ, пов'язані з інформацією та обладнанням для обробки інформації, мають бути ідентифіковані та має підтримуватися їх актуальний інвентарний опис.

Організація повинна виявити активи, що підтримують життєвий цикл інформації, і документально зафіксувати їхню соціальну значимість. Життєвий цикл інформації повинен включати в себе створення, обробку, зберігання, передачу, стирання і знищення. Документація відповідним чином повинна бути зафіксована в спеціально створених або вже існуючих реєстрах.

Реєстр активів повинен бути точним, актуальним, повним і відповідати іншим реєстрам. Для кожного виявленого активу повинен бути призначений власник і має бути проведена класифікація (див. приклад на рис. 4.4).

Рис. 4.4. Приклад вхідної інформації для складання реєстру активів

Реєстри активів сприяють забезпеченню результативного захисту і можуть бути також затребувані для інших цілей, таких як охорона здоров'я та праці, страхування або фінанси (менеджмент активів).

Визначається абсолютна ймовірність та величина витрат. Розглядаються три категорії наслідків: порушення конфіденційності (К), цілісності (Ц) та доступності (Д). Для матеріальних активів збиток визначається за шкалою – від повної втрати активу до збою (зупинки, неполадки) за несуттєвий проміжок часу [14, 15].

Метод VAR

Метод VAR [16] (Value at Risk) заснований на статистичному підході та дозволяє оцінити ризик в термінах можливих втрат співвіднесених з їх ймовірностями виникнення [16]. Тут описується квантиль прогнозованого розподілу втрат протягом певного періоду часу.

Процес оцінювання включає наступні етапи: ідентифікація загроз, оцінка їх ймовірності, обчислення цінності з урахуванням небезпеки та зменшення ризику. Спочатку реалізується класифікація загроз, таких як, наприклад, шахрайство, зловмисні дії, жарти, спроби отримати доступ до приватної інформації, стихійні лиха, саботаж, помилки користувачів та ін. Коли загрози були ідентифіковані, їх ймовірність (розподіл ймовірності) оцінена, можливі сценарії описані, то визначається небезпека для фірми при реалізації загроз [7, 16].

Методика COBRA

Методика COBRA (Consultative Objective and Bi-Functional Risk Analysis, розробник – C & A Systems Security Ltd, Великобританія) орієнтована на підтримку вимог стандарту ISO 17799 за допомогою тематичних опитувальників (check list's) [17]. У комплект ПЗ входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst і COBRA Data Protection Consultant, а також менеджер модуля COBRA, який використовується для налагодження та зміни бази знань.

На основі ініціалізації тематичного опитувальника (ТО) здійснюється АОР за наступними категоріями: високорівнева; IT безпеки; оперативна IT та бізнесу; інфраструктура електронної комерції. Модулі ТО інформаційно підтримують окремі застосунки, наприклад:

– APP-MAN (Application level security management) – управління безпекою;

– APPAUDIT (Application level Auditing) – аудит;

– APPCNTRL (Application Staff control) – контроль штату;
– APPDEPND (Application Staff dependency) – залежність штату;
– AUDIT (System Audit) – перевірка системи та ін.

Після обробки ініціалізованих даних система генерує звіт, в якому описана детальна оцінка (Detailed Risk Assessment (continued)) за такими характеристиками ризику:

– категорія (RISK CATEGORY);
– рівень (RISK LEVEL);
– оцінка (RISK ASSESSMENT).

Відзначимо, що в аналізованій методиці ризик відображається трьома характеристиками, перша та остання з яких несуть в собі ідентифікуючу складову (назва категорії та коментарі до неї), а решта – оціночну складову, якій відповідає «РІВЕНЬ РИЗИКУ», представлений у відсотках (ймовірність настання ризику). Аналіз та ОР відбувається під час обробки даних, ініційованих через ТО. Всі розглянуті дії, які відображаються в запитах, інтегровані в категорії ризику, наприклад, дія розглянута в прикладі запиту входить в категорію ризику «Непередбачувана ситуація в бізнесі (НСБ)». Після опису всіх категорій та ранжирування рівнів ризику (з найвищого до нульового) в методиці наводяться рекомендовані заходи щодо їх зниження.

Метод Coras

Метод Coras (розроблений в рамках програми Information Society Technologies Європейського союзу (SINTEF ICT, Норвегія) використовується для аналізу ризиків безпеки критично важливих систем та реалізується за допомогою технології UML (Unified Modeling Language – уніфікована мова моделювання). Метод орієнтований на підтримку вимог стандартів AS/NZS 4360: 1999 (Risk Management) та ISO/IEC 17799-1: 2000 (Code of Practice for Information Security Management). Засіб оцінювання (метод) ґрунтується на восьми етапах [18] (див. рис. 3.3).

Крок 1 – збір загальної інформації про об'єкт аналізу.

Крок 2 – визначення мети, напрямків та масштабу аналізу.

Крок 3 – деталізація завдань аналізу (див. рис. 3.4).

Крок 4 – аналіз та вивчення отриманої документації.

Крок 5 – визначення ризиків на основі методу «мозкового штурму».

інтересах використати приватну інформацію і комерційні секрети Компанії.

Я підтверджую, що повернув Компанії всі доповіді, креслення, схеми, таблиці та інші письмові та ті, що знаходяться в пам'яті ЕОМ, матеріали і не маю більше в своєму розпорядженні або де - небудь ще таких документів, витягів з них або їх копій.

Дата і підпис службовця

Дата і підпис свідка.

Повернення активів.

Приклад процедури повернення активів:

а) відділ кадрів повідомляє офіцеру з безпеки і керівнику служби IT про надходження заяви на звільнення або на переведення;

б) офіцер з безпеки відповідно до переліку активів, які числяться за працівником, приймає їх від працівника;

в) офіцер з безпеки обстежує робоче місце з метою виявлення додаткових неврахованих активів;

г) служба IT здійснює ревізію і копіювання електронної інформації, що перебуває в користуванні співробітника;

д) офіцер з безпеки візує заяву і повертає її у відділ кадрів.

Видалення прав доступу.

Офіцер з безпеки віддає розпорядження на:

а) заборону (обмеження) фізичного доступу співробітника (Служба охорони);

б) видалення (зміну) прав доступу до інформаційних систем (Управління IT);

в) зміну правил входу і зміну паролів для користувачів, чиї паролі могли бути відомі співробітнику.

4.4. Управління активами

Процес управління активами є однією з найважливіших складових функціонування підприємства як відокремленого господарчого суб'єкта.

У процесі господарської діяльності в розпорядженні підприємства перебувають різні види майна в матеріальній та нематеріальній формі. За економічним змістом майно як активи підприємства поділяють на необоротні та оборотні активи.

Заходи не повинні залежати безпосередньо від фінансового збитку.

Припинення чи зміна умов найму.

Ціль: Захистити інтереси організації як частини процесу зміни умов чи припинення найму.

Припинення чи зміна відповідальності. Має бути чітко визначено, доведено до найманого персоналу чи підрядників і встановлено відповідальності за ІБ та обов'язки, які залишаються дійсними після припинення чи зміни умов найму.

Попередження про припинення трудових відносин має включати в себе інформацію про існуючі вимоги в сфері ІБ та юридичних зобов'язаннях, а також там, де це може бути застосовано, зобов'язання, що випливають з угоди про конфіденційність та умови працевлаштування, що зберігають свою силу протягом певного періоду після завершення трудових відносин зі співробітником або працюючим за контрактом.

Відповідальність і обов'язки, які залишаються в силі після завершення трудових відносин, повинні бути вказані в умовах трудової угоди з співробітником або контракті.

Зміни в посадових функціях чи обов'язки повинні управлятися так само, як і в разі припинення трудових відносин, але доповнені покладанням нових обов'язків і посадових функцій.

Підрозділ з управління персоналом несе загальну відповідальність за процес припинення трудових відносин і взаємодіє з керівником працівника, який звільняється в частині виконання відповідних процедур, що відносяться до ІБ. Якщо мова йде про працівника, який працює за контрактом представника зовнішньої сторони, то процес завершення трудових відносин ведеться зовнішньою стороною відповідно до контракту між нею і організацією.

Можливо, буде потрібно інформувати персонал, споживачів або підрядників про зміни в штатному складі та організаційну структуру [1, 2].

Приклад: Угода про припинення роботи.

Я, що підписався нижче, підтверджую, що був проінструктований щодо комерційних секретів Компанії та її приватної інформації, до якої я мав доступ під час моєї роботи, При прийомі на роботу я підписав угоду про нерозголошення комерційної таємниці і пізніше мене неодноразово попереджали, що я не можу в своїх

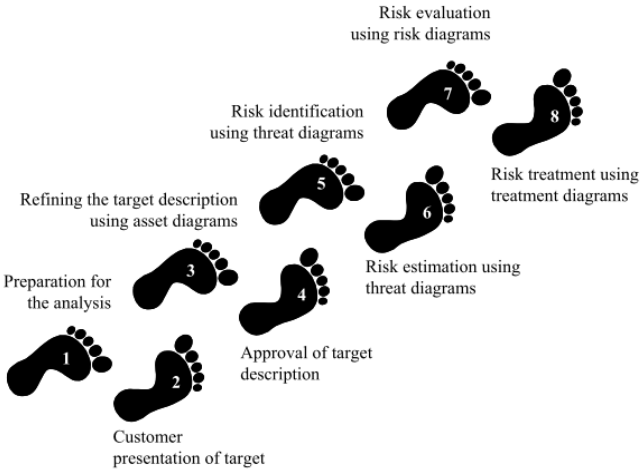


Рис. 3.3. Вісім кроків методу Coras

Крок 6 – визначення рівня ризиків, оцінювання ймовірностей щодо загроз (сценаріїв загроз) та наслідків інцидентів ІБ (див. рис. 3.5).

Крок 7 – визначення прийнятних і неприйнятних ризиків.

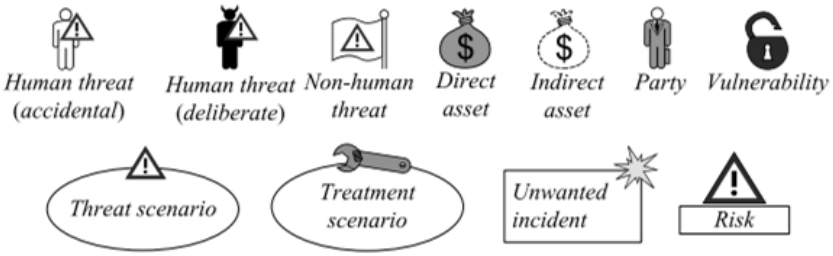


Рис. 3.4. Приклади символів для моделювання ризику

Крок 8 – визначення процедур для усунення загроз з метою зменшення можливої ймовірності (наслідків інцидентів) у сфері ІБ.

Кроки 1-4 є підготовчими, оскільки тут аналітики збирають інформацію про об'єкт аналізу, формують його цілі та шкали для визначення величини ймовірності і наслідків (див. табл. 3.21 і 3.22), а також критерії оцінювання ризиків (див. табл. 3.23). Далі це буде використовуватися для ідентифікації останніх.

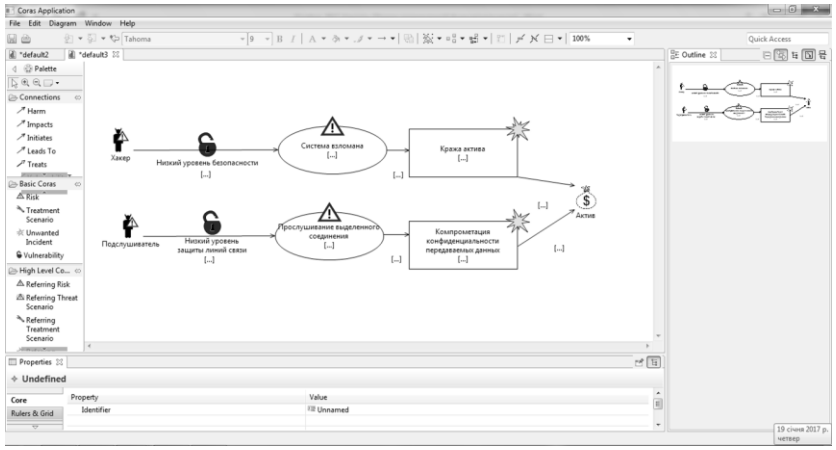


Рис. 3.5. Приклад інтерфейсу інструментарію Coras
(початкова схема загроз для умисних дій)

Таблиця 3.21. Приклад ймовірнісної шкали

Значення ймовірності	Опис	Визначення
Точно	П’ять та більше разів на рік	[50; ∞ 〉 : 10 років = [5; ∞ 〉 : 1 рік
Ймовірно	Від 2 до 5 разів на рік	[20; 50 〉 : 10 років = [2; 5 〉 : 1 рік
Можливо	Менше 2 разів на рік	[5; 20 〉 : 10 років = [0,5; 2 〉 : 1 рік
Навряд	Менше ніж 1 раз на 2 роки	[1; 5 〉 : 10 років = [0,1; 0,5 〉 : 1 рік
Рідко	Менше ніж 1 раз на 10 років	[0; 1 〉 : 10 років = [0; 0,1 〉 : 1 рік

Кроки 5-8 призначені для аналізу і безпосереднього визначення ризиків, їх рівнів (див. табл. 3.23), виявлення та оцінювання потенційних можливостей зменшення неприйнятних ризиків [18].

Таблиця 3.22. Приклад шкали наслідків

Значення наслідків	Кількість ресурсів*
Катастрофічні	>1000
Великі	101÷1000
Середні	11÷100
Низькі	1÷10
Незначні	0
*ресурси, що піддаються впливу	

Метод EBIOS

Метод EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, розробник Національне агентство комп’ютерної безпеки (ANSSI), Центральне управління безпеки

вання, навчання та підготовки повинні відповідати конкретним обов'язкам, відповідальності і навичкам.

У кінці курсу може проводитися оцінювання засвоєння співробітником матеріалу [1, 2].

Підготовка, навчання і тренінг по ІБ.

Головна мета – переконатися в тому, що користувачі:

а) ознайомлені із загрозами порушення режиму ІБ;

б) розуміють значення захисту;

в) мають необхідні навички для виконання процедур, необхідних для нормального функціонування системи безпеки організації.

3) Дисциплінарний процес. Має існувати формальний та офіційно оформлений дисциплінарний процес щодо найманого персоналу, який порушив ІБ.

Дисциплінарні заходи не можуть бути застосовані без попередньої перевірки того, що порушення ІБ дійсно мало місце.

Встановлені дисциплінарні заходи повинні гарантувати коректність і справедливість щодо співробітників, які підозрюються в порушенні ІБ. Встановлені дисциплінарні заходи повинні прийматися як відповідна відповідь, яка враховує такі фактори, як характер і серйозність порушення і його вплив на бізнес, допущено воно в перший раз або повторно, чи був порушник належним чином навчений, наявне відповідне законодавство, бізнес-контракти та інші необхідні фактори.

Дисциплінарні заходи повинні також застосовуватися як профілактичний засіб для запобігання порушенням співробітниками політики та процедур ІБ організації і інших порушень в цій галузі. Навмисно здійснені порушення можуть вимагати негайних дій.

Дисциплінарні заходи можуть також бути мотивуючим або стимулюючим фактором, якщо передбачаються заохочувальні заходи в разі зразкової поведінки в частині ІБ [1, 2].

Заходи повинні бути:

а) розроблені з урахуванням важливості порушення з точки зору здорового глузду;

б) визначені в договорі з працівником;

в) відомі працівнику;

г) виконані у разі виникнення події.

чи заняття в класах, дистанційне навчання, навчання онлайн, самостійні заняття та інші.

Забезпечення поінформованості та підготовка у сфері ІБ повинні також розкривати такі загальні питання, як:

а) прихильність керівництва ІБ;

б) необхідність в ознайомленні і виконанні правил і обов'язків, пов'язаних з ІБ, як це визначено в політиках, стандартах, законах, регламентах, контрактах і угодах;

в) персональна відповідальність за дії або бездіяльність, а також спільна відповідальність щодо безпеки або ЗІ, що належить організації або зовнішнім сторонам;

г) основні процедури ІБ (такі, як звіти з інцидентів ІБ) і основні засоби реалізації (такі, як безпечні паролі, контроль шкідливих програм і політика чистого стола);

д) контакти і ресурси для отримання додаткової інформації та рекомендацій з питань ІБ, включаючи додаткові матеріали для навчання та підготовки у сфері ІБ.

Навчання і підготовка у сфері ІБ повинні проводитися періодично. Початкове навчання та підготовка проводяться для тих, хто переходить на нову позицію або отримує обов'язки з вимогами до ІБ, які істотно відрізняються, а не тільки до тих, хто тільки починає роботу, при цьому навчання має проводитися до того, як співробітник приступить до виконання обов'язків.

Організація повинна розробити програму навчання і підготовки для того, щоб вони проводилися результативно. Програма повинна бути узгоджена з політиками і відповідними процедурами ІБ організації, а також брати до уваги інформацію, яка повинна бути захищена, і заходи, які були вжиті для її захисту. Програма повинна передбачати різні форми навчання і підготовки, наприклад, лекції або самонавчання.

При формуванні програми важливо фокусувати увагу не тільки на «що» і «як», а й «чому». Важливо, щоб співробітники розуміли мету ІБ і можливий вплив – позитивний чи негативний – який чинять на організацію їх дії.

Інформування, навчання і підготовка можуть бути частиною інших навчальних заходів, або виконуватися спільно з ними, наприклад, загальними тренінгами з ІТ або безпеки. Заходи з інформу-

інформаційних систем (DCSSI), Франція) відображає вимоги стандартів ISO/IEC 27001 [19], ISO 31000 [9] та ISO/IEC 27005 [20]. Процес аналізу та оцінювання ризику реалізується за допомогою п'яти модулів.

Таблиця 3.23. Приклад матриці оцінки ризику

Ймовірність	**Наслідки**				
	Незначні	Низькі	Середні	Великі	Катастрофічні
Рідко			CC1, CC1(I)		
Навряд					PR1
Можливо		CI1(I), SS1(I)	CI1, SS1		
Ймовірно				SS2	
Точно					

CC1, CC1 (I) – компрометація конфіденційності, а (I) показує, що ресурс непрямий;
CI1, CI1 (I) – компрометація цілісності; SS1, SS1 (I) – уповільнення системи;
SS2 – неможливість працювати через зависання системи; PR1 – отримання неправильних даних.

Модуль 1 – дослідження контексту. Тут реалізується збір інформації про об'єкт оцінювання за допомогою трьох заходів. Захід 1 – визначення сфери управління ризиками. Захід 2 – підготовка метрик (критерії безпеки (табл. 3.24), рівні небезпеки (табл. 3.25) і ймовірності (табл. 3.26) та критерії управління ризиками).

Таблиця 3.24. Приклад критеріїв безпеки

Критерії безпеки	**Визначення**	**Шкала рівня**	**Детальний опис шкали**
Доступність	Доступність PIC, своєчасність PIC першої необхідності	]72 год.; ∞[	PIC не доступні більше, ніж 72 години
		]24 год.; 72 год.]	PIC доступні протягом 72 годин
		]4 год.; 24 год.]	PIC доступні протягом 24 годин
		]0 год.; 4 год.]	PIC доступні протягом 4 годи
Цілісність	Точність і повнота основних PIC	Виявляються	Зміни PIC ідентифікуються
		Визначаються	Зміни PIC ідентифікуються та визначаються (локалізуються)
		Цілісні	Зміни PIC не здійснюються
Конфіденційність	Основні PIC доступні тільки зареєстрованим користувачам	Відкриті	Публічні
		Обмежені	Доступ тільки для співробітників та партнерів
		Службові	Доступ має тільки персонал, котрий бере участь у розробці
		Персоналізовані	Доступ тільки для конкретних осіб

Захід 3 – ідентифікація ресурсів інформаційних систем (РІС) [21].

Модуль 2 – дослідження небажаних подій. Тут реалізується визначення важливих РІС (з точки зору доступності, цілісності, конфіденційності) та всіх загроз, які можуть призвести до порушення безпеки (їх джерела і ймовірності).

Таблиця 3.25. Приклад шкали небезпек

Шкала рівня	Опис
1. Незначна	Подолання наслідків без будь-яких труднощів
2. Середня	Подолання наслідків незважаючи на низку труднощів
3. Висока	Подолання наслідків з серйозними труднощами
4. Критична	Непереборні наслідки

Модуль 3 – дослідження сценаріїв загроз, яке орієнтоване на виявлення та оцінку сценаріїв, що можуть викликати описані події, які відображають ризики. З цією метою досліджуються джерела загроз та уразливості.Модуль 4 – дослідження ризиків. Тут безпосередньо оцінюються ризики реалізації сценаріїв загроз, які були досліджені у модулі 3.

Таблиця 3.26. Приклад ймовірнісної шкали реалізації сценаріїв загроз

Шкала рівня	Опис
1. Мінімальна	Не має відбутись
2. Середня	Може відбутись
3. Висока	Можливо або точно відбудеться через день-два
4. Максимальна	Відбудеться в найближчий час

Модуль 5 – дослідження заходів безпеки. Модуль орієнтований на визначення заходів безпеки та реалізацію їх тестування [21].

Метод ISAMM

Метод ISAMM (Information Security Assessment & Monitoring Method, розробник Telindus SA (Security, Audit and Governance Services, Бельгія) заснований на вимогах стандарту ISO/IEC 27002. Він ґрунтується на трьох базових компонентах: аналіз об'єкта, оцінка ризику, звітність. Цей кількісний метод оцінювання ризиків ІБ безпосередньо відображає їх через щорічні очікувані збитки в грошових одиницях (Annual Loss Expectancy (ALE)). На перших етапах роботи з методом визначаються загрози ІБ (див. табл. 3.27) [22].

При ОР для кожної загрози (T) оцінюється ймовірність її появи – p_T та очікувані наслідки – I_T .

водити до нехтування ІБ або можливого неправильного застосування активів організації [1, 2].

Головна мета – скорочення кількості порушень.

Керівництво організації повинно регулярно проводити моніторинг виконання вимог з ІБ.

Засобами моніторингу можуть бути:

а) внутрішній аудит СМІБ;
б) аналіз скарг і претензій споживачів;
в) аналіз інцидентів ІБ;
г) періодична атестація персоналу;
д) позачергові перевірки.

2) Поінформованість, освіта й навчання щодо ІБ. Увесь найманий персонал організації, а там, де це суттєво, і підрядники повинні одержати належне навчання й тренінги для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій

Програма з інформування у сфері ІБ повинна бути спрямована на донесення до співробітників і, там, де це суттєво, співробітникам, що працюють за контрактом, їхні обов'язків у сфері ІБ і засобів, якими ці обов'язки можуть бути виконані.

Програма з інформування у сфері ІБ повинна бути узгоджена з політиками і відповідними процедурами ІБ організації, а також брати до уваги інформацію, яка повинна бути захищена, і заходи, які були вжиті для її захисту. Програма повинна включати в себе відповідні інформаційно-агітаційні заходи, наприклад, такі як «день ІБ», випуск брошур або інформаційних листків.

Програма з інформування повинна плануватися з урахуванням тієї ролі, яку відіграють співробітники в організації, і, там, де це суттєво, очікувань організації від обізнаності працюючих за контрактом. Заходи програми повинні бути розраховані на тривалий період, бажано бути регулярними з тим, щоб вони повторювалися і охоплювали нових співробітників і працюючих за контрактом. Програма також повинна регулярно оновлюватися з тим, щоб постійно відповідати політикам і процедурам організації, а також використовувати уроки, добуті з інцидентів ІБ.

Вступний курс повинен проводитися так, як це передбачено програмою з інформування у сфері ІБ організації. Для вступного курсу можуть використовуватися різні методи навчання, включаю-

Я підтверджую, що не маю перед будь-ким ніяких зобов'язань, які суперечать цій угоді або обмежують мою діяльність у Компанії.

Дата і підпис службовця

Дата і підпис свідка.

Рекомендується укладання угод про дотримання режиму ІБ.

Протягом найму.

Ціль: Впевнитися, що весь найманий персонал та підрядники усвідомлюють і виконують свої обов'язки з ІБ.

1) Відповідальність керівництва. Керівництво повинно вимагати від найманого персоналу та підрядників застосування заходів безпеки згідно з установленими в організації політиками та процедурами.

Відповідальність керівництва повинна включати в себе гарантію того, що співробітники і працюючий за контрактом:

а) належним чином поінформовані про свою роль і відповідальність, пов'язаними з ІБ, до того, як отримали доступ до конфіденційної інформації та ІС;

б) забезпечені керівними вказівками, що встановлюють ті очікування щодо ІБ, які пов'язані з їх роллю в організації;

в) мотивовані на виконання політик ІБ організації;

г) обізнані в питаннях ІБ на тому рівні, який відповідає їхній ролі й відповідальності в організації;

д) згодні з умовами зайнятості, які включають політику ІБ організації і відповідні методи роботи;

е) зберігають відповідний рівень навичок і кваліфікацію, а також проходять навчання на регулярній основі;

ж) мають канал для анонімного інформування про порушення політик або процедур ІБ («інформування про порушення»).

Керівництво повинно демонструвати підтримку політик, процедур і засобів управління ІБ, а також діяти відповідно до своєї ролі.

Якщо співробітники і працюючий за контрактом були обізнані про їхню відповідальність у сфері ІБ, це може завдати помітної шкоди організації. Мотивований персонал буде, ймовірно, більш надійним і викликати менше інцидентів ІБ.

Погане управління може привести до того, що персонал буде відчувати себе недооціненим, що може виразитися в негативному впливі на ІБ організації. Наприклад, погане управління може приз-

Таблиця 3.27. Приклад ідентифікованих загроз

ХІБ	ІЗ	Опис
К	С1	Зовнішні зловмисники отримали або отримають доступ до конфіденційної інформації
К	С2	Внутрішні зловмисники отримали або отримають доступ до конфіденційної інформації
К	С3	Випадкове розкриття конфіденційних даних внутрішніми зловмисниками
К	С4	Випадкове розкриття конфіденційних даних зовнішніми зловмисниками
Ц	І1	Модифікація або пошкодження зовнішніми зловмисниками
Ц	І2	Модифікація або пошкодження внутрішніми зловмисниками
Ц	І3	Випадкова, помилкова модифікація
Д	А1	Відмова в обслуговуванні або інші порушення, викликані зловмисниками (шкідливим кодом)
Д	А2	Нестача ресурсів, ноу-хау, підтримка постачальника
Д	А3	Стихійні лиха (землетруси, повені, урагани, блискавки, пожежа, екстремальні погодні умови), терористичні або промислові (ударні) впливи
Д	А4	Відключення системи на короткий період, наприклад, через погодні умови
Д	А5	Ненавмисні відключення через помилки
ХІБ – характеристика ІБ; ІЗ – ідентифікатор загрози; К – конфіденційність; Ц – цілісність; Д – доступність.		

Щорічні очікувані збитки ALE_T для конкретної загрози T визначаються добутком ймовірності виникнення та впливу загрози (див. табл. 3.28):

$$ALE_T = p_T \cdot I_T .$$

Також визначається сумарне значення

$$ALE = \sum_T ALE_T$$

для об'єкта оцінювання [22].

Методологія IRAM$_2$

Методологія IRAM$_2$ (Information Risk Assessment Methodology$_2$, розробник Форум інформаційної безпеки (Information Security Forum), США) реалізується за допомогою шести етапів.

Етап 1 – огляд (пов'язаний з реалізацією аналізу ризиків).

Таблиця 3.28. Приклад оцінювання ризиків

Загроза	Ймовірність (в рік)	Вплив (€)	Поточні ALE_T (€)
C1	1	2000	2000
C2	0,2	2000	400
C3	0,5	400	200
C4	0,5	2000	1000
I1	0,2	50000	10000
I2	0,04	50000	2000
I3	0,5	400	200
A1	0,2	10000	2000
A2	0,2	400	80
A3	0,1	10000	1000
A4	2	400	800
A5	0,5	2000	1000
	Всього	129600	20680

Етап 2 – оцінка впливу (визначення та оцінка різних категорій впливів на бізнес).

Етап 3 – профіль загрози (розробляється модель загроз).

Етап 4 – оцінка уразливостей (виявлення можливостей середовища/системи наскільки добре вона може протистояти загрозам).

Етап 5 – оцінювання ризику (визначається співвідношення ймовірності реалізації загрози та величини її впливу (рис. 3.6)).

Етап 6 – обробка ризику (реалізується розробка планів обробки ризиків) [23].

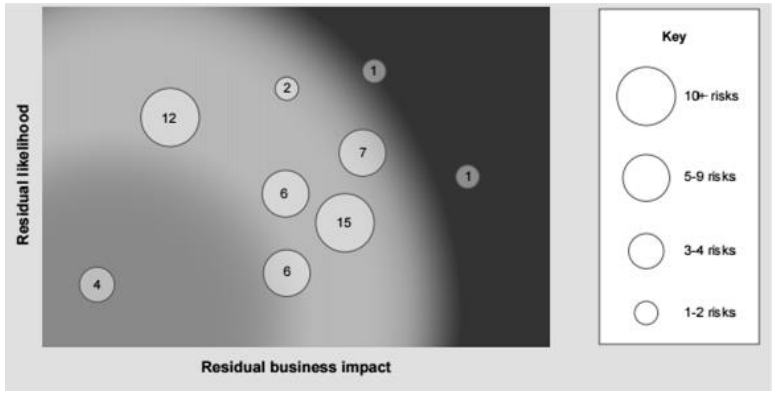


Рис. 3.6. Приклад відображення ризику

відносяться до ІБ, які відповідають характеру і рівню доступу, який вони матимуть до активів організації, пов'язаних з ІС і сервісами.

Там, де це можливо, обов'язки, встановлені положеннями та умовами найму, повинні бути продовжені на певний період і після припинення трудових відносин.

Для встановлення обов'язків співробітника або того, хто працює за контрактом, щодо ІБ, що стосуються конфіденційності, захисту даних, правил поведінки, належного використання обладнання організації, а також очікуваного організацією проходження визнаним практикам, може бути використаний Кодекс поведінки. Зовнішня сторона, з якою пов'язаний працюючий за контрактом, може бути зобов'язана вступати в договірні відносини від імені контрактора [1, 2].

При прийомі на роботу нових співробітників рекомендовано, щоб вони ознайомилися і підписали:

а) письмове формулювання їхніх посадових обов'язків;

б) письмове формулювання прав доступу до ресурсів компанії (в тому числі й інформаційних);

в) угоду про конфіденційність;

г) спеціальні угоди про перлюстрації всіх видів службової кореспонденції (моніторинг мережевих даних, телефонних переговорів, факсів тощо).

Приклад: Угода про нерозголошення комерційної таємниці.

Приступаючи до виконання своїх обов'язків як службовець Компанії, я розумію, що отримаю доступ до інформації, що стосується бізнесу. Я також розумію, що під час роботи буду займатися аналізом, складанням схем, таблиць, креслень, доповідей та інших конфіденційних документів, що відносяться до справ Компанії.

У зв'язку з цим даю зобов'язання, що ні під час моєї роботи, ні після звільнення не буду обговорювати з ким-небудь або розкривати (за винятком випадків виконання своїх обов'язків як службовець Компанії) будь-яку інформацію або комерційні секрети, отримані або розроблені мною . Я також згоден з тим, що всі аналітичні розробки, схеми, креслення, доповіді та інші документи, підготовлені особисто мною або у співпраці з іншими службовцями, є власністю Компанії. Зобов'язуюся, що не буду сам і не дозволю нікому іншому знімати копії або робити анотації з вищезазначених документів.

ній юрисдикції) законодавства. Залежно від чинного законодавства кандидати повинні інформуватися заздалегідь про заходи в межах перевірки.

Аспекти, пов'язані з безпекою, слід враховувати ще на стадії набору персоналу, для цього необхідно:

– включати їх до посадових інструкцій;

– включати їх до договорів;

– контролювати протягом усього часу роботи даного співробітника.

У посадових інструкціях відображена вся характерна даній посаді відповідальність за безпеку.

2) Терміни та умови найму. Контрактна угода з найманим персоналом та підрядниками має встановити взаємні відповідальності щодо ІБ.

Контрактні зобов'язання для співробітників або тих хто працюють за контрактом повинні відображати політики організації щодо ІБ додатково до роз'яснення і встановлення:

а) що всі співробітники й ті, хто працюють за контрактом, хто має доступ до конфіденційної інформації, повинні підписати угоду про нерозголошення конфіденційної інформації до того, як вони отримають доступ до пристроїв обробки інформації;

б) юридичної відповідальності і прав співробітників і тих, хто працюють за контрактом, наприклад, що стосуються законодавства про захист авторських прав або захисту даних.

в) обов'язків із класифікації інформації та управління нею й іншими активами організації, пов'язаними з інформацією, пристроями обробки інформації та інформаційними послугами, використовуваними співробітником або тих хто працюють за контрактом;

г) обов'язків співробітника або того, хто працює за контрактом з обробки інформації, отриманої від інших компаній або зовнішніх сторін;

д) дій, які повинні бути зроблені, якщо співробітник або той, хто працює за контрактом ігнорує вимоги організації з безпеки.

Функції та обов'язки щодо ІБ повинні бути доведені до відома кандидатів на посаду в процесі, що передує прийому на роботу.

Організація повинна гарантувати, що співробітники й ті, хто працюють за контрактом, згодні з положеннями та умовами, що

Система RiskWatch

Система RiskWatch (розробник – компанія RiskWatch, США) відображає вимоги стандартів ISO/IEC 27001 та ISO/IEC 27002, NIST а також COBIT IV. Процес АОР проводиться за чотири фази [24].

Фаза 1 – опис ІС організації з точки зору ІБ (визначення предмета дослідження). Тут описуються такі параметри підприємства, як тип організації, склад досліджуваної системи, базові вимоги в області ІБ.

Фаза 2 – введення даних. Для виявлення уразливостей ініціалізується ТО. Задається частота виникнення кожної з виділених загроз, ступінь уразливості та цінність ресурсів (активів) (рис. 3.7), на підставі чого розраховується ефективність впровадження засобів ЗІ (ЗЗІ) [12].

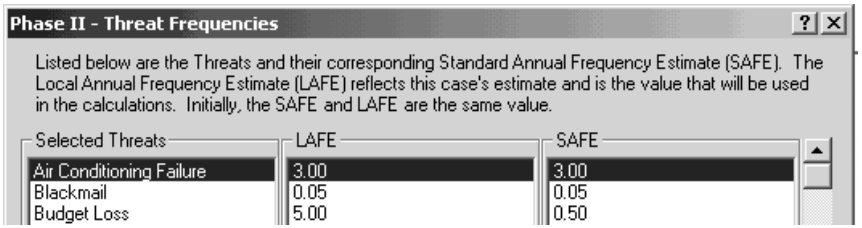


Рис. 3.7. Вікно ініціалізації параметрів

За аналогією з ПЗ COBRA в RiskWatch (для спрощення введення та обробки даних) множини запитів ТО ініціюються за допомогою вибору даних з набору варіантів, наприклад, конкретні числові значення (0, 1 – «ніколи», 2, 3 – «рідко», 4, 5, 6 – «іноді»; 7, 8 – «звичайно»; 9, 10 – «завжди») або «ні», «не знаю». За допомогою запитів відображаються та оцінюються поточні правила ІБ відповідно до існуючих стандартів. Запитом до RiskWatch, наприклад, може бути – «Чи є розмежування доступу до внутрішньої та зовнішньої мережі, точки доступу, окремих комп'ютерів і файлових серверів?» [25].

Фаза 3 – ОР. Розраховується профіль ризиків та вибираються заходи забезпечення ІБ. Для цього встановлюються зв'язки між раніше визначеними ресурсами, втратами, загрозами та уразливостями, а ризик оцінюється за допомогою очікуваних втрат за рік. Наприклад, якщо вартість сервера $v = 150\,000$ \$, а ймовірність його знищення під час пожежі протягом року $p = 0{,}01$, то очікувані втра-

ти складуть $m =$ 1 500 \$, тобто $m = p \cdot v$, де p – ймовірність виникнення загрози, а v – вартість ресурсу. Зазначимо, що RiskWatch базується на таких даних NIST, як LAFE (Local Annual Frequency Estimate) і SAFE (Standard Annual Frequency Estimate), відповідно відображають річну частоту реалізації загроз у локалізованій (наприклад, в місті) та глобалізованій (наприклад, в Північній Америці) областях. Використовується також поправочний коефіцієнт, який враховує часткове знищення ресурсу. Отримання оцінок LAFE та SAFE, наприклад, для України є проблематичним, оскільки відсутня необхідна статистика. Наприклад, в США існує національна програма зі збору даних про інциденти (The Uniform Crime Reporting), що дозволяє сформувати відповідну статистичну інформацію про інциденти ІБ в загальнодержавній базі.

Фаза 4 – генерація звіту (рис. 3.8). Формуються діаграми і таблиці детального відображення відповідності та невідповідності (щодо запитів) вимогам стандарту, а також діаграма втрат.

Theft - Company Property - AFE: 2.00
The various incident classes associated with this threat are shown in the following table:

Incident Class	SLE	ALE	% of total ALE
Delays/Denials, Communications Equipment	$26,401.	$52,801.	68.0%
Delays/Denials, Data/Information	$4,400.	$8,800.	11.3%
Delays/Denials, Physical Inventory/Product	$2,750.	$5,500.	7.1%
Direct Loss, Cash	$2,200.	$4,400.	5.7%
Delays/Denials, Production Resources	$1,100.	$2,200.	2.8%
Direct Loss, Physical Inventory/Product	$1,100.	$2,200.	2.8%
Direct Loss, Data/Information	$550.	$1,100.	1.4%
Direct Loss, Production Resources	$275.	$550.	0.7%
Direct Loss, Communications Equipment	$39.	$77.	0.1%

Рис. 3.8. Фрагмент звіту в RiskWatch

З урахуванням вартості ресурсу здійснюється оцінка очікуваних втрат (за конкретним активом) від реалізації однієї загрози (*ALE*) [12, 26]

$$ALE = A \cdot EF \cdot F,$$

де:

- A – вартість ресурсу (дані, програми, апаратура та ін.);
- EF – коефіцієнт впливу (відсоткова частина від вартості активу, який піддається ризику);
- F – частота виникнення небажаної події.

Наприклад, нехай апаратний засіб коштує A = 10 000 \$, коефіцієнт впливу на нього EF = 0,5, а частота F = 0,2, то очікувані втрати складуть AEL = 1000\$. Після ідентифікації активів та впливів оці-

бізнес-вимогам, категорії інформації за класифікацією, до якої передбачається доступ, і передбачуваним ризикам.

Перевірка повинна проводитися з урахуванням відповідної конфіденційності, захисту персональних даних та трудового законодавства і повинна, де це дозволено, містити наступне:

а) наявність задовільних характеристик, наприклад, однієї від організації і однієї від конкретної особи,

б) перевірка (на повноту і точність) резюме кандидата,

в) підтвердження заявленої освіти і професійної кваліфікації,

г) незалежна перевірка особи (паспорт або інший подібний документ),

д) більш детальна перевірка, наприклад, кредитної історії або наявність кримінального минулого.

Можливе використання тестових методів для виявлення схильності до порушення ІБ.

У тих випадках, коли співробітник приймається на посаду, пов'язану з ІБ, організація повинна переконатися, що кандидат:

а) має необхідний рівень компетентності для цієї посади,

б) гідний довіри на цій посаді, особливо, коли вона критично впливає на організацію.

У тих випадках, коли робота, або доручається спочатку, або в результаті підвищення, вимагає від виконавця наявності доступу до засобів обробки інформації і, особливо, якщо це обробка конфіденційної інформації, наприклад, фінансової, або строго конфіденційної інформації, організація повинна також передбачити більш детальні перевірки.

Процедури повинні визначати критерії та обмеження для перевірок, наприклад, хто має право перевіряти людей і яким чином, коли і чому виконуються перевірки.

Процес перевірки також повинен проводитися і для тих, кого приймають за контрактом. У цьому випадку має бути укладена угода між організацією та тим кого приймають за контрактом, що визначає відповідальність за проведення перевірки та процедури повідомлення, які необхідно виконати, якщо перевірка не була завершена або її результати дають підстави для сумнівів і занепокоєння.

Інформація про всіх кандидатів, розглянутих в організації, повинна збиратися і оброблятися відповідно до чинного (у відповід-

Термін «віддалена робота» відноситься до всіх форм робіт поза офісом, включаючи такі як «telecommuting», «flexible workplace» (гнучке робоче місце), «remote work» і «virtual work» (віртуальне робоче місце) [1, 2].

4.3. Безпека персоналу

Безпека людських ресурсів та захист від загроз пов'язаних з персоналом (див. рис. 4.3).

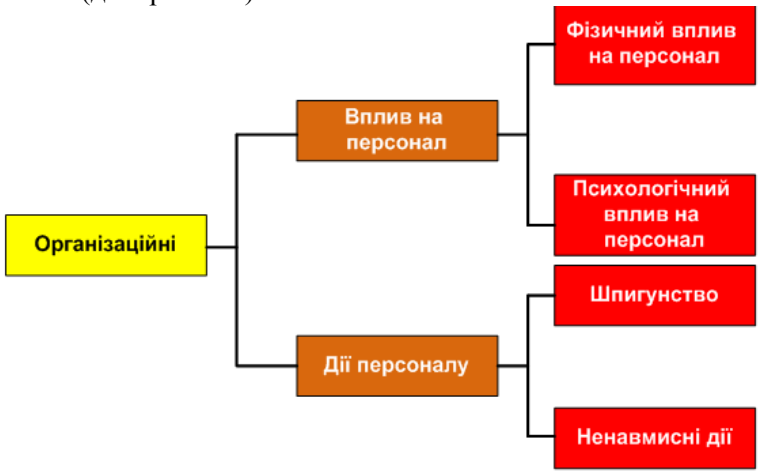


Рис. 4.3. Загрози, пов'язані з персоналом

Перед наймом[8].

Ціль: Гарантувати, що найманий персонал та підрядники розуміють свої обов'язки, придатні до посад, на які претендують.

1) Ретельна перевірка. Підтверджувальні перевірки біографічних даних усіх кандидатів на найм мають виконуватись згідно з усіма відповідними законами, нормативами та морально-етичними нормами, а також співвідносно до бізнес-вимог, класифікації інформації, до якої потрібен доступ, і усвідомлюваних ризиків.

Перевірка при прийомі на роботу, що здійснюється для всіх кандидатів, повинна проводитися в рамках відповідних законодавчих актів, регламентів і етичних норм, а також повинна бути сумірна

[8] Слово «найм» тут призначене, щоб охопити всі різноманітні ситуації: найм людей (тимчасове чи постійне), призначення на посади, зміну посад, підписання контрактів та припинення дії будь-якої з цих угод [1].

нюється загальний ризик для ІС (сума всіх окремих значень). Додатково використовуються показники ARO – очікувана річна частота події та SLE – очікуваний одиничний збиток (різниця початкової та залишкової (після події) вартості активу).

Для оцінювання окремо взятої пари «загроза-ресурс» використовується формула $ALE = ARO \cdot SLE$. Також застосовуються сценарії «що, якщо», що дозволяють описати аналогічні ситуації за умови впровадження засобів захисту.

Порівнюючи очікувані втрати за умови впровадження захисних заходів та без них, можна оцінити ефект від таких заходів. Для цього в RiskWatch містяться не тільки бази даних LAFE та SAFE, але і бази різних СЗІ. Ефект від впровадження засобів безпеки визначається параметром *ROI* – повернення інвестицій, що складає прибуток від вкладень за період часу

Інструментарій RA2 art of risk

Інструментарій RA2 art of risk (RA Software Tool, розробник – компанії AEXIS Security Consultants та XiSEC Consultants Ltd., Великобританія) є ПЗ для реалізації СМІБ, відповідно до вимог ISO/IEC 27001: 2005.

Складається з восьми модулів:

- сфера дії СМІБ та масштаби ОР;
- ідентифікація активів;
- оцінка активів;
- ОЗ/уразливостей;
- ідентифікація та ОР;
- рішення з обробки ризику;
- затвердження застосованих заходів;
- виконання заходів та відбір засобів управління.

В процесі виконання кожного модуля проводиться ініціалізація запитів за допомогою вибору фіксованих значень в бінарно-лінгвістичній формі («так», «ні»). Для ОР використовуються вісім рівнів: 1 – тривіальний; 2, 3 – мінорний; 4, 5 – значний; 6, 7 – великий; 8 – катастрофічний, а матриця ризику будується на основі рівнів небезпеки підприємства та ймовірності ризику в лінгвістичних шкалах. Значення ризику формується у вигляді рівнів за кожною поданою категорією в лінгвістичному та цифровому вигляді, наприклад, значенню «великий рівень» відповідає число 7 [27].

Інструментарій PTA

Інструментарій PTA (Practical Threat Analysis, розробник PTA Technologies, Ізраїль) заснований на вимогах стандарту ISO/IEC 27001 та PCI DSS 1.1 і є програмною системою для розробки моделі загроз, оцінювання ризиків ІБ та складання планів щодо їх зниження. Всі перераховані процеси реалізуються за допомогою чотирьох кроків. Крок 1 – визначення PIC. Тут реалізується ідентифікація PIC із зазначенням їх вартості, пов'язаних з ними загроз, відсоткове співвідношення від загальної вартості всіх PIC системи. Також кожному ресурсу присвоюється ідентифікатор, наприклад, A003 (див. рис. 3.9) [28].

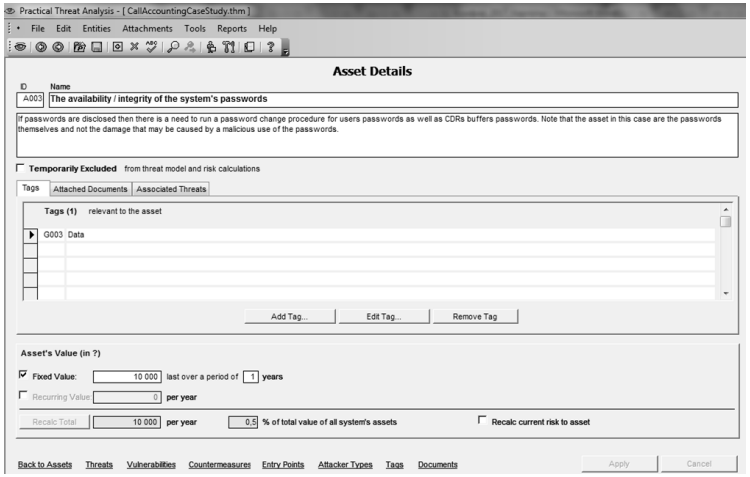


Рис. 3.9. Приклад форми для ідентифікації PIC

Крок 2 – виявлення уразливостей. На цьому кроці аналізуються і фіксуються всі уразливості (рис. 3.10) та загрози, до яких вони можуть призвести.

Рис. 3.10. Приклад форми для фіксування уразливостей

г) надання віртуального робочого столу, який запобігає обробку і збереження інформації на особистому обладнанні;

д) загрозу несанкціонованого доступу до інформації або ресурсів інших осіб, які перебувають у цьому ж приміщенні, наприклад, членів сім'ї чи друзів;

е) використання домашніх мереж і встановлення вимог або обмежень на конфігурацію сервісів бездротових мереж;

ж) політики і процедури для запобігання суперечок щодо прав на інтелектуальну власність, створену на особистому обладнанні;

з) перешкоди для доступу до особистого обладнанню (для перевірки його безпеки або в ході розслідування) законодавчого характеру;

и) ліцензійні угоди на ПЗ, відповідно до яких організація може нести відповідальність за ліцензування клієнтського ПЗ на особистих робочих станціях співробітників або зовнішніх користувачів;

к) вимоги до захисту від шкідливого коду і брандмауерів.

Передбачувані рекомендації і заходи повинні включати в себе:

а) забезпечення відповідним обладнанням та пристроями зберігання для віддаленої роботи в тих випадках, коли застосування особистого обладнання, що знаходиться поза контролем організації, заборонено;

б) визначення дозволених робіт, графіка робіт, категорій інформації, яку можна обробляти, а також внутрішніх системи і сервісів, до яких працівник віддалено має доступ;

в) забезпечення відповідного комунікаційного обладнання, включаючи способи віддаленого безпечного доступу;

г) фізичний захист;

д) правила і рекомендації щодо доступу членів сім'ї та гостей до обладнання та інформації;

е) надання технічної підтримки та обслуговування обладнання і ПЗ;

ж) страхування;

з) процедури резервного копіювання та забезпечення безперервності бізнесу;

и) аудит і моніторинг безпеки;

к) припинення повноважень і прав доступу, а також повернення обладнання при завершенні віддалених робіт.

Мобільні пристрої для бездротових з'єднань схожі на інші типи пристроїв з'єднання з мережами, але мають важливі відмінності, які повинні бути враховані при визначенні засобів управління. Типовими відмінностями є:

а) деякі протоколи захисту для бездротових комунікацій недосконалі і мають відомі уразливості;

б) інформація, що зберігається на мобільних пристроях, не може бути збережена у вигляді резервної копії в силу обмеженості пропускної здатності мережі або ж тому, що мобільний пристрій не приєднаний до мережі в ті моменти часу, коли за розкладом відбувається резервне копіювання.

Мобільні пристрої здебільшого мають загальні функції зі стаціонарно використовуваними пристроями, наприклад, робота в мережі, доступ до Інтернету, електронну пошту та управління файлами. Засоби управління ІБ для мобільних пристроїв, зазвичай, включають в себе ті ж самі, що застосовуються і для стаціонарно використовуваних пристроїв, а також ті, що спрямовані на захист від загроз, пов'язаних з використанням пристроїв поза приміщеннями організації.

2) Віддалена робота. Політика та заходи підтримання безпеки мають бути запроваджені для ЗІ, яка доступна, обробляється чи зберігається в місцях віддаленої роботи.

Повинні бути прийняті політика і заходи забезпечення безпеки для ЗІ, до якої здійснюється доступ на віддалених робочих місцях і яка там обробляється або зберігається.

Організації, що практикують віддалену роботу, повинні розробити політику, яка визначає умови й обмеження для дистанційної роботи. Там, де це може бути застосовано і допустимо з точки зору закону, може бути прийнято до уваги наступне:

а) наявний рівень фізичного захисту віддаленого місця роботи з урахуванням фізичного захисту будівлі та місцевих умов;

б) пропоновані фізичні умови віддаленої роботи;

в) вимоги до безпеки комунікацій, беручи до уваги необхідність віддаленого доступу до внутрішніх систем організації, ступінь важливості інформації, до якої буде здійснюватися доступ, і яка буде передаватися по каналах зв'язку, а також уразливість внутрішньої системи;

Крок 3 – визначення контрзаходів. Цей крок передбачає вибір контрзаходів для перекриття уразливості і запобігання реалізації загроз (див. рис. 3.11 та 3.12). Також реалізується ОР як співвідношення ймовірності реалізації загрози та шкоди від її реалізації (рис. 3.11) [28].

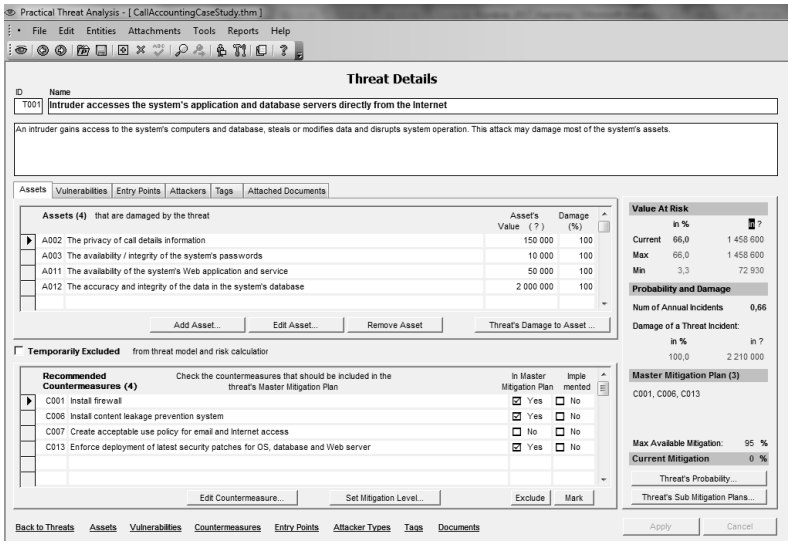


Рис. 3.11. Приклад форми для фіксування загроз та оцінювання ризику

Крок 4 – розробка планів нейтралізації сценаріїв загроз (рис. 3.13) [28].

Система КЕС управління ІБ «АванГард»

Система КЕС управління ІБ «Авангард» (Комплексна експертна система «Авангард», розробник – Лабораторія системного аналізу проблем інформатизації Інституту системного аналізу РАН, Росія) включає комплекс методик:

− ідентифікації критично важливих сегментів та об'єктів інформаційної інфраструктури на основі АОР порушення ІБ автоматизованих ІС (АІС);

− управління ризиками порушення ІБ великих комп'ютеризованих організаційних систем;

− побудови системи вимог ІБ критично важливих сегментів та об'єктів АІС;

– моніторингового контролю над станом критично важливих сегментів та об'єктів AIC.

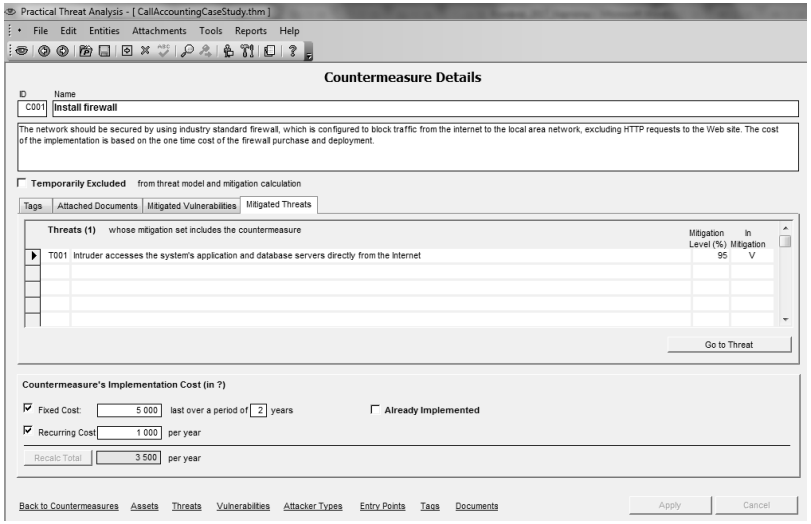


Рис. 3.12. Приклад форми для фіксування контрзаходів

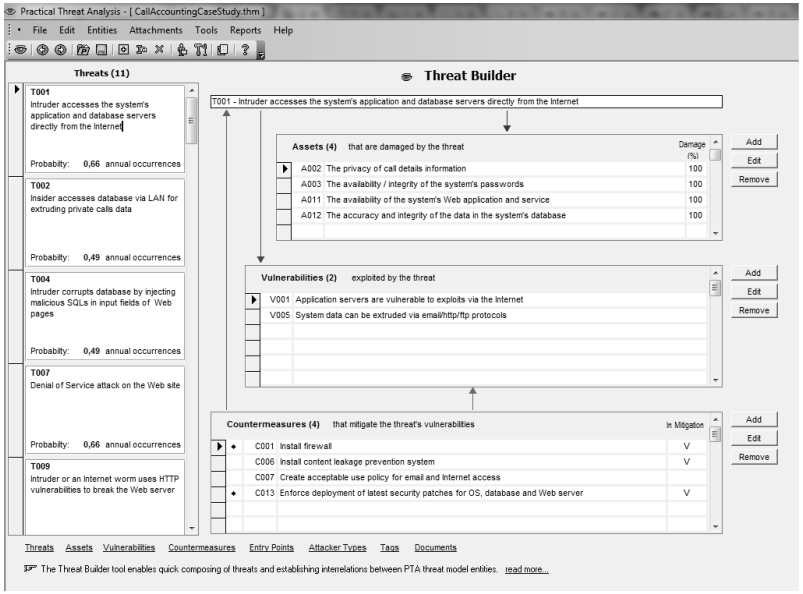


Рис. 3.13. Приклад взаємозв'язку PIC, уразливостей, загроз та контрзаходів

Можливі наслідки для ІБ повинні враховуватися і аналізуватися регулярно у всіх проектах. Обов'язки з ІБ повинні бути визначені і пов'язані з конкретними посадами в рамках прийнятої методології управління проектом.

Мобільне обладнання та віддалена робота:

Гарантувати безпеку віддаленої роботи та використання мобільного обладнання.

1) Політика щодо мобільного обладнання. Політика та заходи підтримання безпеки мають бути пристосовані до управління ризиками, які виникають через використання мобільного обладнання.

Повинні бути прийняті політика і заходи щодо забезпечення безпеки для управління ризиками, пов'язаними з використанням мобільних пристроїв.

При використанні мобільних пристроїв особлива увага повинна бути приділена гарантії того, що не буде розголошена інформація, яка представляє комерційну таємницю. Політика щодо мобільних пристроїв повинна брати до уваги ризики використання мобільних пристроїв в незахищених середовищах.

Політика щодо мобільних пристроїв повинна передбачати:

а) реєстрацію мобільних пристроїв;
б) вимоги щодо фізичного захисту;
в) обмеження на установку ПЗ;
г) вимоги до версій програм і застосовуваним патчам;
д) обмеження на користування інформаційними послугами;
е) контроль доступу;
ж) криптографічні технології;
з) захист від шкідливого коду;
и) віддалене вимикання, стирання або блокування;
к) резервне копіювання;
л) використання веб-сервісів і веб-додатків.

Необхідно дотримуватися обережності при використанні мобільних пристроїв в громадських місцях, конференц-залах і інших незахищених місцях. Повинний бути забезпечений захист, щоб уникнути несанкціонованого доступу або розкриття інформації, яка зберігається або обробляється пристроями, наприклад, застосуванням криптографічних методів і примусовим застосуванням секретної інформації для автентифікації.

д) публікації та обміну інформацією про нові технології, продукти, загрози або уразливості;

е) забезпечення відповідних контактів при обробці інцидентів ІБ.

Для поліпшення співпраці і координації у питаннях безпеки можуть формуватися угоди про обмін інформацією. Такі угоди повинні визначати вимоги до захисту конфіденційної інформації.

Приклад роботи з безпеки в угодах із третіми особами.

Приклад: Угода про збереження комерційної інформації.

Тут і далі «Довіритель» або Ваше ім'я, тут і далі «Довірений» бажають розглянути можливість _____, для чого необхідно, щоб Довірений мав доступ до інформації _____

Ця інформація становить комерційну таємницю Довірителя і розкривається тільки в заздалегідь обумовлених цілях. Довірений зобов'язується зберігати в секреті цю інформацію і не використовувати її в інших цілях. Довірений зобов'язується ознайомити під розпис з цією угодою всіх своїх співробітників, які отримають доступ до цієї інформації. Після закінчення переговорів (або співпраці) Довірений відразу ж поверне всі матеріали, що містять дану інформацію, Довірителю.

Ця угода не стосується інформації, законним власником якої є Довірений, або інформації, отриманої ним від третіх осіб.

Дата Підпис.

5) ІБ в управлінні проектами. ІБ потрібно брати до уваги під час управління проектами незалежно від типу проекту.

Заходи щодо забезпечення ІБ повинні бути інтегровані в методи управління проектами в організації, щоб гарантувати, що ризики ІБ виявлено та опрацьовано в рамках проекту. Це відноситься зазвичай до будь-якого проекту незалежно від його характеру, наприклад, проектам для основного бізнес-процесу, ІТ, обслуговування устаткування та іншим процесам, які підтримуються. Застосовувані методи управління проектами повинні передбачати, що:

а) цілі ІБ включені в цілі проекту;

б) оцінювання ризиків ІБ проводиться на ранній стадії проекту для визначення засобів управління;

в) ЗІ є частиною всіх етапів застосовуваної методології проекту.

Засновується система на двох програмних комплексах – «Авангард-Аналіз» і «Авангард-Контроль» [29]. Спочатку проводиться аналіз подій ризику через побудову їх моделей за допомогою інтерфейсу головної форми (рис. 3.14), де у верхньому секторі міститься таблиця зі списком моделей подій ризиків, за кожною з яких в заданих графах зазначаються експертні оцінки ціни ризику (в умовних одиницях) та ймовірності (у відсотках) його подій.

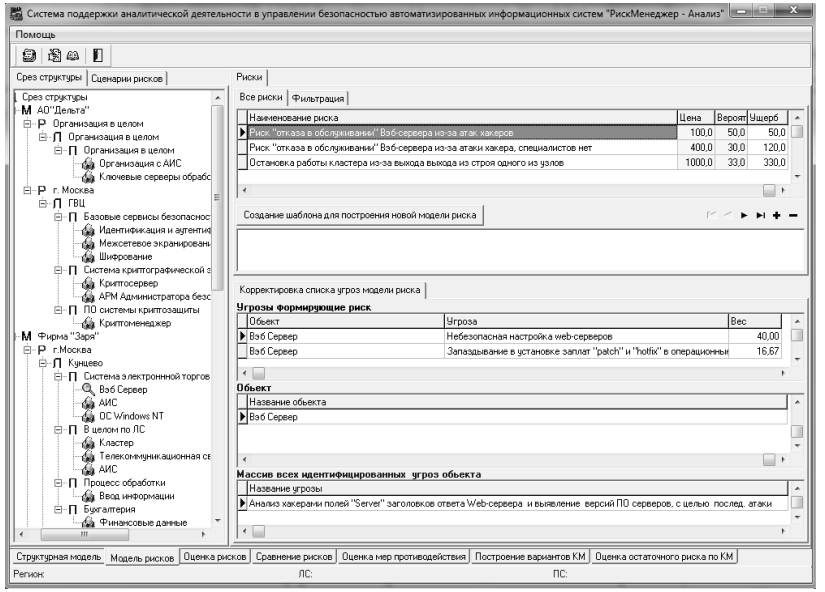


Рис. 3.14. Інтерфейс побудови моделей подій ризику

При матеріальній шкоді умовної одиниці рекомендується привласнювати певний ціновий еквівалент, наприклад, 1000 руб.

При події ризику, збиток від якого складно оцінити в грошовому еквіваленті, використовуються бальні оцінки, за якими ранжуються події ризику відповідно до ступеню їх небезпеки. У графі «Збиток» ідентифікується розрахункове значення ризику за добутком його ціни на ймовірність.

У наступному секторі представлена таблиця загроз, реалізація яких пов’язана з певним ризиком. Для кожної із загроз зазначається вага заданої події (ризикоутворюючий потенціал (РП) загрози за подією ризику). Для оцінки необхідно:

− вибрати клас об'єкта з описом дії, яка призводить до ризику (визначити його ідентифікатор);

− для кожного ризику встановити грошовий еквівалент;

− розглянути події ризику, які можуть виникнути в результаті реалізації цих загроз (для визначення значущості загроз, які входять до складу нормативної моделі) [29].

Система Enterprise Risk Assessor

Система Enterprise Risk Assessor (Risk Advisor, розробник – компанія Methodware, Нова Зеландія) відповідає вимогам австралійського стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360: 1999) та ISO/IEC 17799.

Представлена в трьох продуктах: CobiT Advisor 3rd Edition (Audit); PRo Audit Advisor; Planning Advisor. Процес АОР проводиться за три кроки, що дозволяє структурувати оцінку, зробити її більш точною.

Крок 1: Додаток The Builder Tool – інструмент для створення структури ОР і аудиту (збір інформації). Воно дозволяє побудувати структуру ІС, включаючи здатність додавати або приховувати будь-яку частину функціональних можливостей. Основні етапи роботи в цьому додатку складаються з опису ІС, ризиків, загроз, втрат та аналізу результатів.

На етапі «Опис ризику» створюється матриця (рис. 3.15), яка дозволяє описати ризики відповідно до визначеного шаблону та сформувати їх зв’язок з іншими елементами моделі. Оцінювання відбувається на основі якісної шкали, а ризики поділяються на прийнятні та неприйнятні. Далі вибираються управляючі впливи (контрзаходи) з урахуванням зафіксованої раніше системи критеріїв, ефективності контрзаходів та їх вартості. Вартість і ефективність також оцінюються в якісних шкалах.

На етапі «Опис загроз» спочатку визначається список загроз, здійснюється їх класифікація та формується зв'язка з ризиками. Опис також робиться на якісному рівні, що дозволяє зафіксувати їх взаємозв'язки.

На етапі «Опис втрат» описуються події (наслідки), пов'язані з порушенням режиму ІБ. Втрати оцінюються в обраній системі критеріїв. Для спрощення збору даних експерти можуть використовувати ТО, який складається вручну. Після збору інформації переходимо до ОР.

3) Контакти з повноважними органами. Необхідно підтримувати належні контакти з відповідними повноважними органами.

Організації повинні мати процедури, які визначають, коли і через кого буде здійснюватися контакт з повноважним органом (наприклад, правоохоронними органами, контролюючими та наглядовими органами) і яким чином виявлена інформація з інцидентів ІБ буде своєчасно передаватися (наприклад, якщо є підозра на можливе порушення закону).

Організації, які зазнали атаки через Інтернет, можуть мати необхідність звернення до повноважних органів для вжиття заходів проти джерела атаки.

Підтримка таких контактів може бути вимогою, що забезпечує управління інцидентами ІБ, або безперервність бізнесу і процес планування дій у надзвичайній ситуації. Контакти з контролюючими органами також корисні з точки зору раннього інформування та підготовки до передбачуваних змін в законодавстві або нормативних вимогах, які організації повинні будуть виконати. Інші повноважні органи, з якими можуть підтримуватися контакти, включають в себе комунальні та аварійні служби, постачальників електроенергії, служби порятунку, наприклад, пожежних (у світлі безперервності бізнесу), телекомунікаційних провайдерів (у плані маршрутизації і доступності), а також служби водопостачання (у плані забезпечення роботи охолоджувальних пристроїв для обладнання).

4) Контакти з групами фахівців з певної проблематики. Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об’єднаннями.

Членство в професійних співтовариствах або форумах повинно розглядатися як засіб для:

а) розширення знань про кращі практики і отримання самої найновішої інформації у сфері ІБ;

б) гарантії того, що уявлення про аспекти ІБ є актуальним і повним;

в) раннього отримання попереджень про небезпеку, інформаційних бюлетенів та патчів, що стосуються атак і уразливостей;

г) забезпечення можливості отримання порад від фахівців з ІБ;

Сфера, за які відповідають призначені особи, повинні бути визначені. Зокрема має бути зроблено наступне:

а) виявлені і визначені активи та процеси забезпечення ІБ;

б) повинна бути призначена відповідальна особа для кожного активу або процесу забезпечення ІБ, повинна бути документально підтверджена деталізована інформація, що стосується цієї відповідальності;

в) повинні бути визначені і документовані рівні повноважень;

г) для забезпечення здатності нести відповідальність в сфері ІБ призначені особи повинні бути компетентними в цій галузі і їм повинна бути забезпечена можливість розвитку для підтримки своєї компетентності на потрібному рівні;

д) повинні бути визначені і документовані підходи до координації та контролю ІБ в рамках взаємодії з постачальниками.

Багато організацій покладають на менеджера ІБ загальну відповідальність за розробку і впровадження засобів ЗІ, за забезпечення вибору засобів управління. При цьому відповідальність за виділення ресурсів і реалізацію засобів управління буде часто залишатися у конкретних керівників. Одна із загальноприйнятих практик полягає в тому, щоб кожному активу призначати власника, який потім буде відповідальним за щоденний його захист.

2) Розподіл обов'язків. Конфліктуючі обов'язки та сфери відповідальності мають бути розподілені для зменшення можливостей неавторизованої чи ненавмисної модифікації або неправильного використання ресурсів СМІБ організації.

Необхідно стежити за тим, щоб одна і та ж особа не могло мати доступ, змінювати або застосовувати актив без авторизації або впізнання. Ініціювання події повинно бути відокремлене від його авторизації. При розробці засобів управління повинна враховуватися можливість змови.

Для невеликих організацій поділ обов'язків може становити певні труднощі в реалізації, проте, сам принцип повинен застосовуватися настільки повно, наскільки це можливо і практично доцільно. Там, де є труднощі з розподілом обов'язків, повинні застосовуватися інші методи реалізації, такі як моніторинг дій, аудити та контроль керівництва.

Розподіл обов'язків є методом зниження ризику випадкового або навмисного неправильного застосування активів організації.

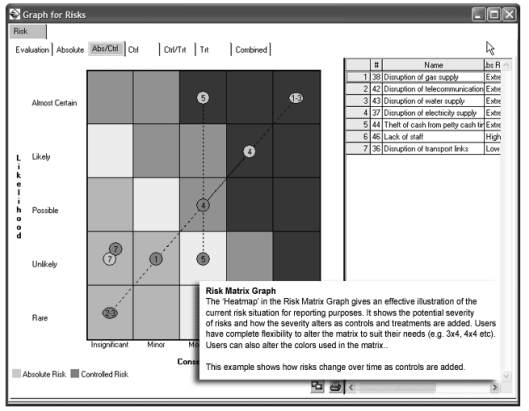


Рис. 3.15. Матриця ризику

Крок 2: The Assessor – експертна оцінка (аналіз зібраної інформації).

Крок 3: The Consolidation Tool – інструмент консолідації (інтегрує всі індивідуальні ОР). Після побудови моделі формується звіт (близько 100 розділів) та агрегований опис у вигляді графа ризиків [27, 30]. У звіті (рис. 3.16) з ймовірносно-лінгвістичною шкалою ризик представлений у вигляді матриці з такими градаціями: майже напевно, ймовірно, можливо, малоймовірно, рідко. На рис. 3.17 представлено приклад опису та ОР.

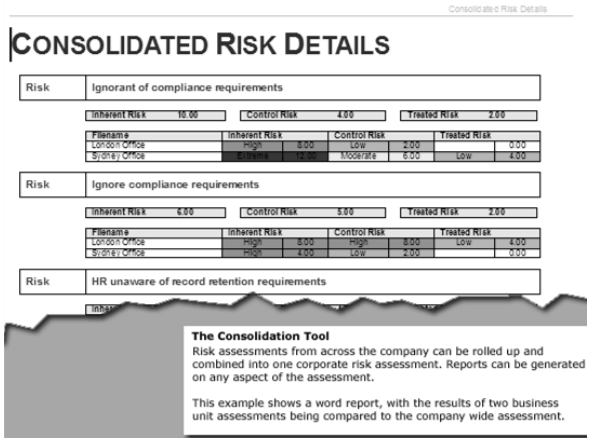


Рис. 3.16. Фрагмент звіту

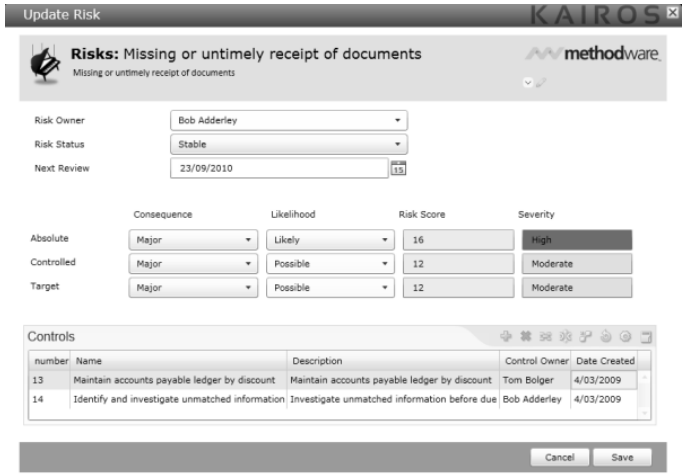


Рис. 3.17. Приклад опису ризику

Система vsRisk, Risk Assessment Tool

Система vsRisk, Risk Assessment Tool (розробник – компанія Vigilant Software Ltd., Великобританія) призначена для ОР ІБ відповідно до вимог ISO/IEC 27001 та BS 7799-3. Для спрощення процедури АОР використовуються форми, для яких вибираються шкали (встановлюються рівні) ймовірності та впливу. Далі, для кожної дії визначається ймовірність за обраною шкалою (рис. 3.18, а). Система надає засоби для оцінки всіх чинників ризиків, включаючи загрози, уразливості, активи та механізми контролю, і не містить засобів для кількісної оцінки величини ризику, обмежуючись лише якісними шкалами.

Відзначимо, що для оцінювання задаються масштаби ймовірності та впливу розглянутих загроз. Всі зміни, що вносяться до бази даних продукту в ході роботи, докладним чином фіксуються в журналі аудиту. Після аналізу ризиків формується оцінка у вигляді обраного балу для ймовірності, наприклад, 2. За результатами оцінки генеруються «Декларації про можливість застосування механізмів контролю» та «План обробки ризиків» відповідно до вимог стандарту ISO/IEC 27001. Надалі ця інформація використовується при наданні рекомендацій на відповідність цьому стандарту. У vsRisk немає детальної ОР з описом подальших дій, що рекомендуються (рис. 3.18, б) [31].

17) Політика видалення ПЗ;
18) Політика захисту і секретності даних.

Усі ці політики підкріплюють:

– ідентифікацію ризику шляхом надання основи засобів управління, які можуть використовуватися для виявлення недоліків у проектуванні та впровадженні систем;

– обробку ризику шляхом надання допомоги у визначенні способів обробки для певних уразливостей і загроз.

Ідентифікація ризику і обробка ризику – це процеси, визначені в розділі політики «Принципи».

Подробиці див. у політиці СМІБ [3].

4.2. Організаційне забезпечення інформаційної безпеки

Внутрішня організація:

Цілі. Визначити структуру управління для започаткування і контролю впровадження та функціонування ІБ в організації.

Завдання: Сформувати основні елементи управління для ініціювання, контролю впровадження та експлуатації засобів ЗІ в організації.

1) Ролі та обов'язки щодо ІБ. Усі обов'язки щодо ІБ необхідно чітко визначити та розподілити. Повинні бути визначені і призначені всі обов'язки, пов'язані з ІБ.

Призначення обов'язків, пов'язаних з ІБ, має проводитися відповідно до політиками ІБ (див. підрозділ 4.1). Повинні бути визначені обов'язки:

– пов'язані із захистом конкретних активів і виконанням конкретних процесів ЗІ;

– для дій з управління ризиками і, особливо, для прийняття остаточних ризиків. Ці обов'язки повинні забезпечуватися підтримкою, якщо необхідно, у вигляді більш детальних інструкцій для конкретних ділянок і пристроїв обробки інформації;

– на місцях для захисту активів і виконання конкретних процесів ЗІ.

Особи, яким визначено обов'язки, пов'язані з безпекою інформації, можуть делегувати виконання завдань щодо захисту іншим особам. Але в будь-якому випадку вони залишаються відповідальними і повинні переконуватися, що будь-яке делеговане завдання виконано належним чином.

2) Кожен керівник вищої ланки відповідає за те, щоб співробітники, що працюють під його керівництвом, здійснювали ЗІ відповідно до стандартів організації.

3) Начальник відділу безпеки консультує групу керівників вищої ланки, надає експертну допомога співробітникам організації й забезпечує доступність звітів про стан ІБ.

4) Кожен співробітник організації відповідає за ІБ, це як частина виконання своїх посадових обов'язків.

Ключові результати

1) Інциденти ІБ не повинні призводити до серйозних непередбачених витрат або серйозних зривів роботи служб і діяльності підприємства.

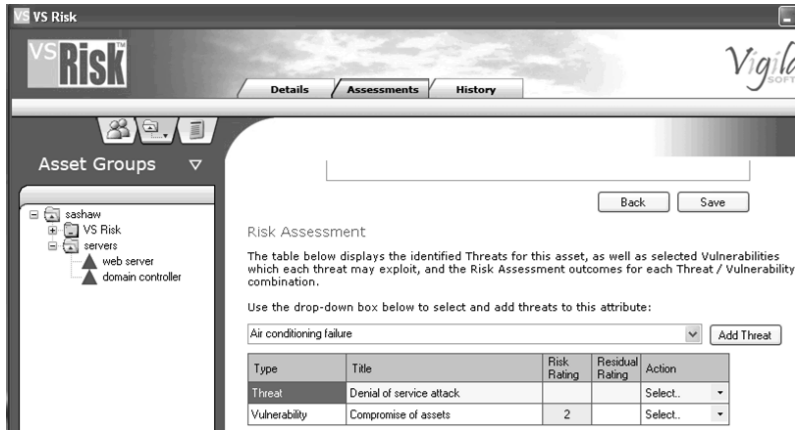
2) Втрати через шахрайство повинні бути відомі і перебувати в рамках прийнятних обмежень.

3) Питання ІБ не повинні мати негативного впливу на прийом замовниками продукції і послуг.

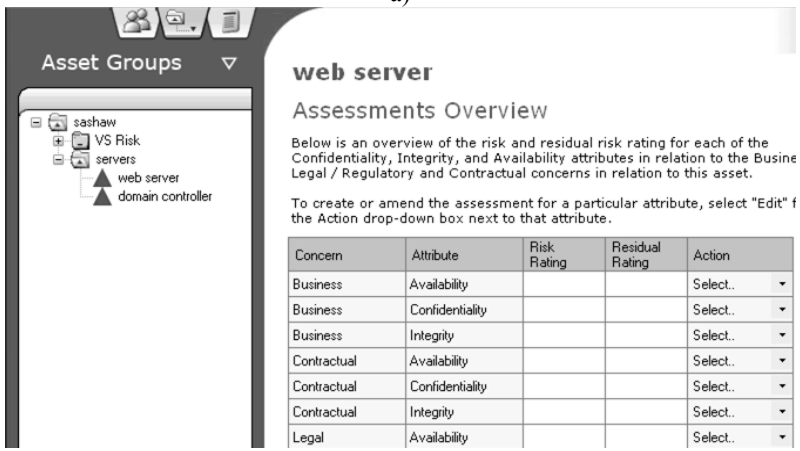
Пов'язані політики

Наступні детальні політики містять принципи і рекомендації щодо окремих аспектів ІБ:

1) Політика СМІБ;
2) Політика контролю доступу;
3) Політика «чистого столу» та «чистого екрану»;
4) Політика недозволеного ПЗ;
5) Політика, що стосується отримання файлів ПЗ з зовнішніх мереж або через них;
6) Політика, що стосується мобільного коду;
7) Політика резервного копіювання;
8) Політика, що стосується обміну інформацією між організаціями;
9) Політика, що стосується допустимого використання електронних засобів зв'язку;
10) Політика збереження записів;
11) Політика використання мережевих служб;
12) Політика, що стосується мобільних обчислень та зв'язку;
13) Політика дистанційної роботи;
14) Політика використання криптографічного контролю;
15) Політика відповідності;
16) Політика ліцензування ПЗ;



а)



б)

Рис. 3.18. Приклад роботи системи:
а) фрагмент інтерфейсу OP; б) короткий огляд оцінок

Система OCTAVE

Система OCTAVE (розробник – інститут Carnegie Mellon Software Engineering Institute і Центр навчання, досліджень і технологій (CERT), реалізований в лінійці продуктів: метод OCTAVE, OCTAVE-S та OCTAVE Allegro – для великих, середніх і малих організацій відповідно, США) використовує трьохетапний підхід для вивчення організаційних та технічних питань.

Етап 1 – «Ідентифікація активів та уразливостей». Складається з чотирьох процесів:

− «Ідентифікація ресурсів управління» (збирається інформація про важливі активи, вимоги ІБ, загрози та уразливості від представників компанії);

− «Ідентифікація експлуатаційних ресурсів» (збирається інформація, як в попередньому процесі, з відібраних експлуатаційних сфер);

− «Ідентифікація ресурсів штату» (збирається інформація аналогічно з попередніми процесами від загального штату відібраних експлуатаційних сфер);

− «Створення профілів загроз» (вибирається 3 ÷ 5 критичних ресурсів, для яких і визначаються профілі загроз).

Для проходження цього етапу в системі пропонується ініціювати ТО (рис. 3.19, *а*).

Container Type	Questions to Consider
Technical (*see* **Worksheet 9a**)	*Internal* ❑ What information systems use or process this information asset? *Example:* • *The vendor database (information asset) is used by the accounts payable system (system).* ❑ What automated processes are reliant on this information asset? *Example:* • *Paying an invoice (process) requires information in the vendor database (information asset) and is automated in the accounts payable system (system).* ❑ On what hardware might this information asset be found? Consider: • If the information asset is used by a system, application, or process, what underlying hardware is related to the information asset? *Examples:* • *The vendor database is stored on the "DIAMOND" server.* *External*

а)

Інформаційна безпека – це захист інформації від різних загроз, покликана забезпечити безперервність бізнес-процесів, мінімізувати ризик для бізнесу і максимізувати повернення вкладень та забезпечити можливості ділової діяльності.

Сфера дії

Ця політика підкріплює загальну політику безпеки організації. Ця політика застосовується до всіх співробітників організації.

Цілі інформаційної безпеки

1) Розуміння і обробка стратегічних і оперативних ризиків для ІБ, щоб вони були прийнятні для організації.

2) Захист конфіденційності інформації клієнтів, розробок продукції і планів маркетингу.

3) Збереження цілісності матеріалів бухгалтерського обліку.

4) Відповідність загальних веб-сервісів і внутрішніх мереж відповідним стандартам доступності.

Принципи ІБ

1) Така організація сприяє прийняттю ризиків і долає ризики, які не можуть подолати організації з консервативним управлінням, за умови розуміння, моніторингу та обробки ризиків для інформації при необхідності. Детальний опис підходів, що застосовуються для оцінювання та обробки ризиків, можна знайти в політиці СМІБ.

2) Весь персонал повинен бути обізнаний і підзвітний за ІБ у відношенні своїх посадових обов'язків.

3) Необхідно вжити заходів для фінансування засобів управління ІБ і процесів управління проектами.

4) Можливості шахрайства та зловживань в області ІБ повинні бути взяті до уваги при загальному управлінні ІБ.

5) Звіти про стан ІБ повинні бути доступні.

6) Необхідно відслідковувати ризики для ІБ та вживати заходів, коли зміни призводять до виникнення непередбачених ризиків.

7) Критерії класифікації ризиків і прийнятності ризиків можна знайти в політиці СМІБ.

8) Ситуації, які можуть привести організацію до порушення законів і встановлених норм, не повинні допускатися.

Сфери відповідальності

1) Група керівників вищої ланки відповідає за забезпечення відповідного опрацювання інформації в усій організації.

Політики можуть мати наступну структуру:

1) Короткий виклад політики – загальний опис з однієї-двох пропозицій. (Іноді може об'єднуватися зі вступом).

2) Вступ – коротке пояснення предмету політики.

3) Сфера дії – описує частини або дії організації, що знаходяться під впливом політики. При необхідності в пункті «Сфера дії» перераховуються інші політики, підкріплені даною політикою.

4) Цілі – опис призначення політики.

5) Принципи – опис правил, що стосуються дій і рішень для досягнення цілей. В деяких випадках може бути корисним визначити ключові процеси, пов'язані з предметом політики, і потім – правила виконання процесів.

6) Сфери відповідальності – хто відповідає за дії з виконання вимог політики. В деяких випадках цей пункт може містити опис організаційних угод, а також сфери відповідальності осіб з певними ролями.

7) Ключові результати – опис результатів, одержаних підприємством при досягнені мети.

8) Пов'язані політики – опис інших політик, які відносяться до досягнення цілей, зазвичай з поданням додаткових подробиць, що стосуються окремих предметів.

Зміст політики може бути організовано різними способами, наприклад, організації, які роблять акцент на ролях і сферах відповідальності, можуть спростити опис цілей і застосовувати принципи конкретно до ролей і сфер відповідальності.

Нижче наведено приклад політики ІБ, що показує її структуру і зміст.

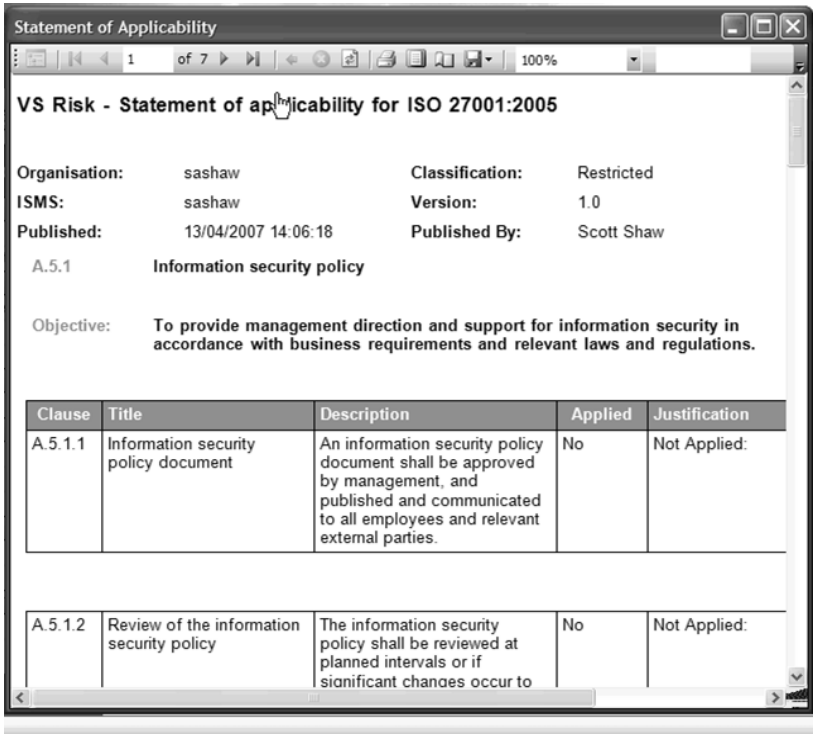
Політика ІБ (приклад)

Короткий виклад політики

Інформація завжди повинна бути захищена незалежно від її форми і способу її поширення, передачі та зберігання.

Вступ

Інформація може існувати в багатьох різних формах. Вона може бути надрукована або написана на папері, зберігатися в електронному вигляді, передаватися поштою або з використанням електронних пристроїв, показуватися на плівках або передаватися усно в процесі спілкування.



б)

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	8
Financial	5	Low (1)	5
Productivity	3	Low (1)	3
Safety and Health	1	Low (1)	1
Fines/Legal	2	High (3)	6
		Total Score	**23**

в)

Рис. 3.19. Приклад роботи системи:
а) фрагмент запитів для етапу 1; б) звіт відповідності;
в) результат оцінки загального ризику

Етап 2 – «Ідентифікація загроз та уразливостей інфраструктури». Містить два процеси:

– «Ідентифікація ключових компонент» (складається представницький набір ключових компонент системи, які підтримують або обробляють критичні інформаційно-пов'язані активи);

– «Оцінка відібраних компонент» (проводиться оцінка відібраних компонент та аналіз результатів (рис. 3.19, б)).

Загрози поділяють на такі категорії:

– за участю людини і використанням технічних засобів; за участю людини і використанням фізичного доступу;

– технічні проблеми та інші проблеми.

В процесі проходження етапу 2 ризик визначається як функція $R(T,I)$, де T – загроза (threat)/умова (condition), а I – вплив (impact)/наслідок (consequence). Також детально описується збиток, який буде завдано компанії в разі настання ситуації ризику.

Етап 3 – «Розвиток стратегії та планів безпеки» (ідентифікуються ризики до критичних активів організації та приймаються рішення з їх обробки). Складається з двох процесів:

– «АОР» (визначається рівень впливу (високий, середній, низький) загроз критичним активам);

– «Розвиток стратегії захисту» (команда розвиває стратегію захисту всієї організації, зосереджуючись на поліпшенні методів забезпечення її ІБ [32]).

Приклад процесу оцінювання (при цьому використовується шкала – середній, низький, високий) щодо заданої сфери дії ризику розглянуто в табл. 3.29. Надалі при загальній оцінці для кожної сфери присвоюється коефіцієнт рівня ризику:

– високий – 3,

– середній – 2,

– низький – 1.

Отримані бали щодо кожної загрози в процесі АОР підсумовуються (рис. 3.19, в).

Таблиця 3.29. Приклад процесу ОР

Сфера діяльності ризику	Рівень ризику
репутація/довіра клієнтів	середній
фінанси	низький
виробництво	низький
безпека та здоров'я	низький
штрафи	високий

Рис. 4.1. Ієрархія політики

Зміст політики засновано на контексті, в якому працює організація. Зокрема, при розробці будь-якої політики в рамках основ політики потрібно враховувати наступне:

1) цілі і завдання організації;

2) стратегії, адаптовані для досягнення цих цілей;

3) структуру і процеси, адаптовані організацією;

4) цілі і завдання, пов'язані з предметом політики;

5) вимоги пов'язаних політик вищого рівня.

Цей процес показаний на рис. 4.2.

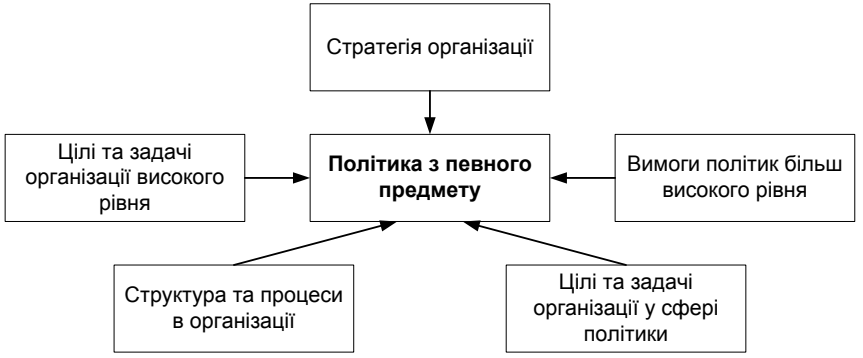


Рис. 4.2. Вихідні дані для розробки політики

Перегляд політик ІБ. Політики ІБ для гарантії їх постійної придатності, відповідності та результативності повинні переглядатися через заплановані інтервали часу або в разі істотних змін.

Кожна політика повинна бути закріплена за «власником», що має підтверджену керівництвом відповідальність за розробку, перегляд та оцінку політик. Перегляд повинен включати оцінку можливостей для покращення політик організації і підходу до управління ІБ у відповідь на зміни в оточенні організації, діловому середовищі, законодавстві або технічній галузі.

Перегляд політик ІБ має здійснюватися з урахуванням результатів аналізу менеджменту.

Результати перегляду повинні бути затверджені керівництвом [2].

Політика ІБ.

1) Може ґрунтуватися на Концепції з Безпеки, Концепції з ІБ, Політики у сфері якості, Вимог стандарту ISO 27001;
2) Можлива наявність двох політик;
3) Повинна(і) бути документально підтверджена(і);
4) Затверджена(і) керівництвом;
5) Повинна(і) переглядатися.

У сфері безпеки політики переважно ієрархічно організовані. Зазвичай ПБ організації є політикою вищого рівня. Вона підкріплюється більш конкретними політиками, включаючи політику ІБ і політику СМІБ. У свою чергу, політика ІБ може підкріплюватися більш детальними політиками з конкретних предметів, що належать до аспектів ІБ. Багато з цих політик описуються в стандарті ISO / IEC 27002, наприклад, політика ІБ підкріплюється політиками, що стосуються контролю доступу, політики «чистого столу» та «чистого екрану», використання мережевих служб і криптографічного контролю. У деяких випадках можливе включення додаткових рівнів політики. Ця класифікація показана на рис. 4.1.

Відповідно до стандарту ISO / IEC 27001 потрібно, щоб організації мали політику СМІБ і політику ІБ. Однак це не визначає будь-яких конкретних співвідношень між цими політиками. Ці політики можуть розроблятися як рівноправні політики: політика СМІБ може підпорядковуватись політиці ІБ, або, навпаки, політика ІБ може підпорядковуватись політиці СМІБ.

Інструментарій Callio Secura 17799

Інструментарій Callio Secura 17799 (розробник – компанія Callio Technologies, Канада) є Web-додатком, який включає все необхідне для менеджера при розробці, впровадженні, управлінні та сертифікації СМІБ згідно ISO/IEC 17799 / BS7799 [33]. Система містить чотири секції:

– «Методологія» – помічник, який пояснює кроки правильного здійснення впровадження ISO/IEC 17799 та просування до сертифікації BS 7799-2;

– «Адміністрування» – інструментарій для правильного визначення структури управління СМІБ;

– «Інструменти» – набір інструментів для реалізації правильного виконання вимог ISO/IEC 17799;

– «Управління ІБ» – модулі, що дозволяють ефективно управляти ризиками організації та підготуватися до аудиту СМІБ. Для ОР ІБ необхідно ініціалізувати ТО, складений відповідно до вимог стандарту [34].

Процес АОР здійснюється за два етапи. На першому – реалізується ідентифікація активів, загроз, уразливостей та вимог ІБ, оцінюється величина уразливостей, ймовірність загроз та цінність активів, яка визначається збитком в результаті порушення конфіденційності, цілісності, доступності (рис. 3.20). З використанням цих даних обчислюється значення ризику [34].

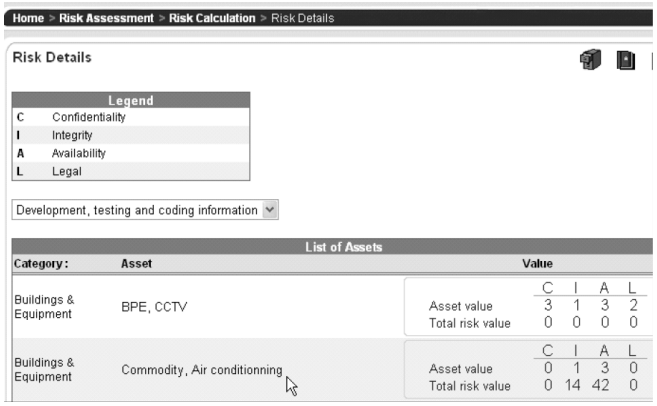


Рис. 3.20. Приклад ОР

На другому етапі приймається рішення щодо способів обробки ризиків та прийнятного рівня залишкових ризиків, створюється план обробки ризиків, проводиться впровадження механізмів контролю і розробки політики ІБ та інших організаційно-розпорядчих документів.

Під час опису необхідно поставити дані щодо критеріїв «високий» – (3), «середній» – 2), «низький» – (1) [35]. Базуючись на інформації про цінності активів і ймовірності загроз, автоматично обчислюються значення ризиків та проводиться їх упорядкування за пріоритетами (ризик щодо конфіденційності, цілісності, доступності та законності).

Система Гриф 2006

Система Гриф 2006 (розробник – компанія Digital Security, Росія) спрямований на забезпечення самостійної роботи IT-менеджера (без залучення сторонніх експертів) щодо оцінки РР в ІС та ефективності існуючої практики із забезпечення безпеки компанії, а також надання можливості доказово (в цифрах) переконати керівництво в необхідності інвестицій в сферу ІБ. Процес АОР в системі Гриф 2006 складається з 3 етапів.

Етап 1 – складання моделі аналізу інформаційних потоків (опис активів компанії та всіх бізнес-процесів).

Етап 2 – створення моделі аналізу загроз та уразливостей. Для оцінки використовується розроблена Digital Security класифікація загроз, в якій описані всі дії, що розглядаються під час оцінювання, здатні призвести до порушення базових характеристик ІБ, тобто до подій порушення ІБ.

Етап 3 – зазначення шкоди для кожної групи цінних ресурсів, за всіма видами загроз. На цьому етапі необхідно ініціалізувати ТО з політики ІБ, реалізованої в системі, що дозволить оцінити реальний рівень її захищеності та деталізувати ОР. Аналіз ризиків ІБ здійснюється за допомогою побудови моделі ІС організації [12].

Ризик оцінюється окремо за кожною зв'язкою «група користувачів – інформація», тобто модель розглядає взаємозв’язок «суб'єкт – об'єкт» з урахуванням всіх їх характеристик.

Розраховуються ймовірність реалізації загрози, її рівень щодо уразливості на основі критичності та ймовірності реалізації через дану уразливість і можливі збитки. В системі використовується шкала від 0 до 100%.

певних цільових груп в організації або за певними цільовими сферами.

Як приклад, такі цільові області можуть включати:

а) контроль доступу;
б) класифікацію (і обробку) інформації;
в) фізичний захист і захист від природних факторів;
г) цільові області, орієнтовані на кінцевого користувача, такі як:
   1) належне використання активів;
   2) принцип чистого столу і чистого екрану;
   3) передача інформації;
   4) мобільні пристрої і віддалена робота;
   5) обмеження на установку й використання програм;
д) резервне копіювання;
е) передача інформації;
ж) захист від шкідливого коду;
з) управління технічними уразливостями;
и) криптографічні методи;
к) безпеку обміну інформацією;
л) конфіденційність і захист персональних даних;
м) відносини з постачальниками.

Ці політики мають бути доведені до відома співробітників і відповідних зовнішніх сторін у адекватній, доступній і зрозумілій передбачуваній читачеві формі.

Необхідність у внутрішніх політиках різниться в різних організаціях. Внутрішні політики особливо корисні у великих і складних за структурою організаціях, де ті, хто визначає і затверджує очікуваний рівень управління, відокремлені від тих, хто реалізовує засоби управління, або в ситуаціях, коли політика поширюється в організації на багатьох людей або на багатьох різних функцій. Політики ІБ можуть бути зведені до загального документу – «політика ІБ» або утворювати комплект окремих, але пов'язаних документів.

При передачі політик ІБ за межі організації слід стежити за тим, щоб при цьому не була розкрита конфіденційна інформація.

Деякі організації використовують інші терміни для документів, що містять, політику, наприклад, «стандарт», «положення» або «правила».

Розділ 4. ЗАСОБИ РЕАЛІЗАЦІЇ ТА ПІДТРИМКИ ФУНКЦІОНУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Політики інформаційної безпеки

Вище керівництво повинно запровадити політику ІБ, яка:

а) відповідає цілям організації;

б) містить цілі ІБ або зазначає основні положення для визначення цілей ІБ;

в) містить зобов'язання відповідати застосованим вимогам, пов'язаним з ІБ;

г) містить зобов'язання щодо постійного вдосконалення СМІБ.

Політика ІБ має:

а) бути доступною як документована інформація;

б) бути розповсюдженою в середині організації;

в) бути доступною зацікавленим сторонам, за потреби.

Мета ПБ. Забезпечити принципи управління та підтримку ІБ згідно з вимогами бізнесу та відповідними законами й нормативами.

Набір політик щодо ІБ повинен бути визначений, затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та потрібних зовнішніх сторін.

Політики ІБ потрібно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності й ефективності [1].

Політики ІБ повинні враховувати вимоги, що випливають з:

а) бізнес стратегії;

б) законодавства, регламентів і контрактів;

в) існуючих і прогнозованих загроз ІБ.

Політики ІБ повинні містити положення, що стосуються:

а) визначення ІБ, цілей і принципів для керівництва всіма діями, пов'язаними з ІБ;

б) призначення загальних і конкретних обов'язків з менеджменту ІБ певним посадам;

в) процесів обробки відхилень і винятків.

На нижньому рівні політика ІБ повинна розкриватися в політиках за відповідними напрямами, які далі реалізуються в засобах управління ІБ та, як правило, поділяються відповідно до потреб

Система @RISK

Система @RISK (розробник – компанія Palisade, США) призначена для АОР за допомогою методу Монте-Карло [36], що реалізується на основі Microsoft Excel. Система дозволяє простежити можливість прийняття та уникнення ризиків, а також приймати найкращі рішення в умовах невизначеності. Для ОР також використовується метод Value at Risk (VAR) [16].

На початковому етапі роботи проводиться створення моделі оцінки (аналіз ризику) за допомогою заповнення таблиці (див. приклад табл. 3.30). Далі відбувається розрахунок витрат при настанні ситуації порушення ІБ.

Таблиця 3.30. Приклад таблиці експлуатаційних ризиків

Експлуатаційні ризики	Ймовірність (річна) %	Вплив ($)	Середній вплив ($)
Відмова ІТ системи	0,1	1000	5
Проблема з виробничим процесом	0,05	50	3
Тяжке захворювання члена правління	0,05	100	5
Службовець виграє судовий процес	0,08	250	20
Поява нового конкурента	0,25	400	100
Відмова випуску нового товару	0,15	300	45
Закріплення ставки $	0,35	100	35
Пожежа в головному офісі	0,02	250	5
Шахрайство	0,005	500	3
Втрата конфіденційних даних	0,01	300	3
Банкротство головного клієнта-боржника	0,02	150	3
Загальна кількість		**3400**	**227**

Система RiskPAC

Система RiskPAC (розробник – компанія CSCI, Нідерланди) призначена для виявлення та надання допомоги в усуненні уразливостей в ІС. Конструктор анкет дозволяє автоматизувати будь-яку ручну методику ОР для аналізу якого необхідно ініціалізувати (за допомогою фіксованих варіантів) запити в ТО, представлених у вигляді реляційних баз даних (БД). Під час ОР для підрахунку ймовірності загроз використовується наступна шкала: малоймовірно, ймовірно та

цілком ймовірно. Також підраховується вплив за шкалою: мінімальний, значний, серйозний та катастрофічний. Додатково в системі є калькулятор очікуваних середньорічних втрат [30, 37].

Система Microsoft Security Assessment Tool

Система Microsoft Security Assessment Tool (MSAT, розробник – компанія Microsoft, США) базується на матеріалах «Керівництва з управління ризиками» [38]) та виконує наступні функції:

1) ОР;
2) підтримка прийняття рішень;
3) реалізація контролю;
4) оцінка ефективності програми.

Програмний застосунок орієнтований на організації з числом співробітників менше 1000 чоловік для сприяння кращому розумінню потенційних проблем у сфері ІБ. В ході роботи користувач, який виконує роль аналітика відповідального за питання ІБ, працює з двома групами запитів.

Перша з них присвячена ОР для бізнесу, з яким компанія стикається в даній галузі та в умовах обраної бізнес-моделі. Створюється так званий профіль ризику для бізнесу. Запити цієї групи розбиті на 6 етапів:

Етап 1 – «Параметри компанії» (назва, кількість комп'ютерів та серверів і тощо);
Етап 2 – «Безпека інфраструктури»;
Етап 3 – «Безпека застосунків»;
Етап 4 – «Безпека операцій»;
Етап 5 – «Безпека персоналу»;
Етап 6 – «Середовище».

Після реалізації етапів цієї групи здійснюється обробка (за допомогою підключення до інтернет) отриманої інформації та перехід до другої групи запитів, які організовані відповідно до концепції багаторівневого (ешелонованого) ЗІ. Багато в чому ТО відповідає розділам стандартів ISO/IEC 17799 та ISO/IEC 27001.

Після ініціалізації запитів клієнтська частина програмної системи знову звертається до віддаленого сервера та генерує звіти. Найбільший інтерес представляє «Повний звіт», що містить пропонований список пріоритетних дій. На етапі аналізу ризику проводиться ідентифікація активів, пропонується їх якісна класифікація (високий, середній та низький вплив на бізнес), а також визначається

62) «Vulnerabilities» [Electronic resource], SecurityFocus, Mountain View, 2016 [Online]. Access mode: http://www.securityfocus.com/ -53r4 – Falls Church: Natl. Inst. Stand. Technol, 2013, p. 462.

63) «A Complete Guide to the Common Vulnerability Scoring System. Version 2.0», [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/v2/guide.

64) «Common Vulnerability Scoring System v3.0: User Guide» [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss /user-guide.

65) «Компания Positive Technologies: Оценка уязвимостей CVSS 3.0», [Электронный ресурс], HABRAHABR Сообщество IT-специалистов, Москва, 2016, [Online]. Режим доступа: https://habrahabr.ru/ company/ pt/blog / 266485/.

66) «CWE™ International in scope and free for public use», [Electronic resource], MITRE, Bedford, 2016, [Online]. Access mode: http://cwe.mitre.org/index.html.

67) «X-Force – команда исследователей и разработчиков IBM Internet Security Systems (ISS)», [Электронный ресурс], IBM Corporation, New York, 2016, [Online]. Режим доступа: https://www.ibm.com/ru/services/iss/research.html

68) «Методи захисту системи управління інформаційною безпекою», Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП «УкрНДНЦ», 2016, с. 28.

69) Т. Крет, «Методика опису інформаційних активів організації при створенні системи менеджменту інформаційної безпеки», «Computer science & Engineering 2011» (CSE-2011), 24-26 november 2011, lviv, Ukraine, p. 342-343.

средах», Безопасность информационных технологий, № 4, С. 68-74, 2014.

52) А. Урзов, С. Варлатая, «Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности», Доклады ТУСУРа, № 2 (28), С. 142-146, 2013.

53) А. Федорченко, А. Чечулин, И. Котенко, «Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей», Информационно-управляющие системы, №5 (72), С. 72-79, 2014.

54) А. Федорченко, А. Чечулин, И. Котенко, «Построение интегрированной базы уязвимостей», Известия высших учебных заведений. Приборостроение, Т.57, №11, С. 62-67, 2014.

55) В. Харченко, Алаа Мохаммед Абдул-Хади, Ю. Поночовный, «Формирование подмножеств уязвимостей доступности коммерческих Веб-сервисов», Системи обробки інформації, випуск 7 (114), С. 112-115, 2013.

56) А. Белобородов, А. Горбенко, «Применение баз данных уязвимостей в задачах исследования безопасности программных средств», Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка, Вип. 165, С. 83-85, 2015.

57) «National Vulnerability Database» [Electronic resource], National Institute of Standards and Technology, Gaithersburg, 2016, [Online]. Access mode: https://nvd.nist.gov/home.cfm.

58) «Банк данных угроз безопасности информации» [Электронный ресурс], Федеральной службой по техническому и экспортному контролю России, Москва, 2016, [Online]. Режим доступа: http://bdu.fstec.ru/.

59) «Open Sourced Vulnerability Database» [Electronic resource], Open Security Foundation, Lafayette, 2016, [Online]. Access mode: https:// http://osvdb.org/

60) «IBM X-Force Exchange» [Electronic resource], IBM Corporation, New York, 2016, [Online]. Access mode: https:// exchange. xforce. ibmcloud.com/ vulnerabilities/109429.

61) «Vulnerability Notes Database» [Electronic resource], United States Computer Emergency Readiness Team, Murray Lane, 2016, [Online]. Access mode: https://www.kb.cert.org/vuls/#

перелік загроз та уразливостей. На етапі ОР визначається потенційний збиток за трирівневою шкалою (висока, середня та низька схильність до впливу).

При оцінюванні частоти виникнення загроз використовуються градації:

– висока (ймовірне виникнення одного або декількох подій в межах року);
– середня (вплив може виникнути в межах двох-трьох років);
– низька (виникнення впливу в межах трьох років малоймовірно).

Методика TRA

Методика TRA [39, 40] (Threat and Risk Assessment, розробник – компанія Government (Communications Security Establishment), Канада) розроблена на основі трьох посібників для ІТ-систем з:

– сертифікації та акредитації (MG-01);
– управління ризиком безпеки (MG-02);
– ОР і вибору гарантій (MG-03 [40]).

Для ОР аналітик повинен розглянути опис ІТ-системи, ідентифікувати істотні сценарії загроз, оцінити вплив та їх ЙВ (рис. 3.21).

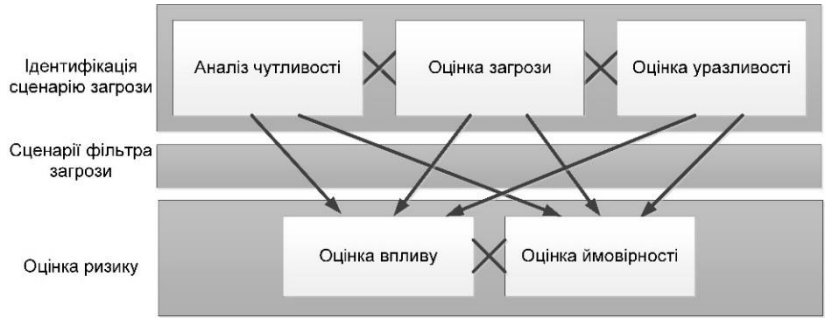


Рис. 3.21. Процес ОР

В процесі ОР для кожного сценарію загрози розраховуються її вплив та ймовірність. Такий підхід відображає середні очікувані втрати за певний період часу [39]. По суті, ризик (R) описується як функціональний зв'язок між вартістю активів (A_{Val}), загрозою (T) та уразливістю (V): $R = f(A_{Val}, T, V)$.

Процес ОЗ (наприклад, «Хакерська атака») для такої підгрупи активів як корпоративні дані (КД) здійснюється на основі табл. 3.31

[39], де рівень порушення таких характеристик ІБ, як К, Ц та Д відображається трирівневою КЛ шкалою («В», «С», «Н»).

Таблиця 3.31. Приклад ОЗ

Клас загрози	Дія загрози	Категорія агента загрози (АЗ)	АЗ	Подія загрози	Рівень порушення			Підгрупа активів
					К	Ц	Д	
Навмисна	Шпіонаж	Хакери	-	НСД	В	-	-	КД
	Саботаж	Хакери	-	НСМ	-	-	В	КД
	Саботаж	Хакери	-	DoS	-	Н	-	КД

Методика FRAP

Методика FRAP [41] (Facilitated Risk Analysis Process, розробник – компанія Peltier and Associates, США) орієнтована на забезпечення ІБ ІС, яка розглядається в рамках процесу управління ризиками та складається з п'яти етапів:

Етап 1 – Визначення активів, які захищаються (проводиться на основі ТО, вивчення документації на систему, використання інструментів автоматизованого аналізу (сканування) мереж).

Етап 2 – Ідентифікація загроз. При складанні списку загроз можуть використовуватися різні підходи, наприклад:

- вибір актуальних для даної ІС загроз із заздалегідь підготовлених експертами переліків (checklists);
- аналізується статистика інцидентів ІБ, пов'язаних з даною ІС;
- оцінюється середньорічна частота інцидентів (за низкою загроз, наприклад, виникнення пожежі, дані можна отримати у відповідних державних організаціях);
- фахівці компанії вирішують завдання за допомогою «мозкового штурму» та ін.

Етап 3 – ОР. Кожній загрозі зі складеного списку зіставляють її ЙВ, далі оцінюють збиток, який може бути нанесений даною загрозою та за отриманими значеннями оцінюється її рівень. При проведенні аналізу ризику, як правило, приймають, що на початковому етапі в системі відсутні засоби та механізми захисту. Таким чином оцінюється РР для незахищеної ІС, що надалі дозволяє показати ефект від впровадження засобів ЗІ. Оцінювання проводиться за ЙВ загрози та шкоди від її реалізації протягом року з використанням наступних шкал. Для ймовірності (Probability):

40) «A Guide to risk assessment and safeguard selection for Information Technology Systems», MG-3 K1G 3Z4, Ontario: Government of Canada, Communications Security Establishment (CSE) P.O., 1996, p. 65.

41) T. Peltier, Information security risk analysis, London, Auerbach Publications, 2001, p. 281.

42) W. Rowe, An anatomy of risk, NY: John Wiley, 1997, p. 488.

43) Anderson, Alison Shain, Michael Shain, «Anderson Risk Management», Information Security Handbook, New York: Stockton Press, P. 75–127, 1991.

44) «MEHARI – Overview», Club de la Securit ´ e de l'Information Franc¸ais, Paris: CLUSIF, 2010, p. 50.

45) «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. Book I», The Method, [version 2], Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006, p. 140.

46) М. Гарсия, Проектирование и оценка систем физической защиты, М., Мир, 2002, с. 386.

47) «MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. II», Catalogue of Elements, [version 2], Madrid : MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006, p. 87.

48) «CMS Information Security Risk Assessment (RA) Methodology», [CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)] Baltimore : Centers for Medicare & Medicaid Services, 2002, p. 21.

49) Е. Скулыш, А. Корченко, Ю. Горбенко, С. Казмирчук, «Средства анализа и оценки риска информационной безопасности», Інформаційна безпека. Людина, суспільство, держава, №3 (7), С. 31-48, 2011.

50) С. Казмирчук, А. Охрименко, «Анализ и оценка риска потер государственных информационных ресурсов», Інтегровані інтелектуальні робототехнічні комплекси (ІІРТС 2012) = Integrated Intellectual Robotechnical Complexes (IIRTC 2012), П'ята міжнар. наук.-практ. конф. : тези доп., К.: НАУ, 2012, С. 325–326.

51) А. Малюк, А. Царегородцев, Е. Макаренко, «Один из подходов к оценке рисков информационной безопасности в облачных

31) «Compliant Information Security Risk Assessment Tool: vsRisk», [Electronic resource], IT Governance Ltd., Boise : IT Governance Ltd, 2011. [Online]. Access mode: http://www.27001.com/products/31.

32) C. Alberts, S. Behrens, R. Pethia, W. Wilson, OC-TAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM), Hanscom : SEI Joint Program Office, 1999, p. 72.

33) «Information technology. Security techniques. Code of practice for information security management. International standard», ISO/IEC 17799:2005, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2005, p. 115.

34) «Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799)» [Электронный ресурс], Callio Technologies, М.: Представительство Callio Technologies, 2012, [Online]. Режим доступа: http://businesssoft.ru. – Загл. с экрана [просмотрено 18 марта 2011].

35) «Consultative Committee for Space Data Systems. Guide for secure system interconnection informational report», CCSDS 350.4-G-1, Washington: Green book November, 2007, p. 51.

36) А. Лукашов, «Монте-Карло для аналитиков. Как грамотно моделировать и измерять риски», Риск-менеджмент, №3, С. 73–77, 2007.

37) «Inventory of risk assessment and risk management methods», [Reference document], Paris: Securing Europe's Information Society Regulation, 2004, p. 460.

38) «Руководство по управлению рисками безопасности» [Электронный ресурс], Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам; Центр Microsoft security center of excellence, TechNet, Редмонд, США: Корпорация Майкрософт, 2006, [Online]. Режим доступа: http://technet.microsoft.com/ru-ru/library/cc163143.aspx. – [просмотрено 29 декабря 2011].

39) A. Syalim, Y. Hori, K. Sakurai, «Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide», International Conference on Issue, Fukuoka: Grad. Sch. of Inf. Sci. & Electr. Eng, P. 726–731.

– висока (High Probability) – ймовірно;
– середня (Medium Probability) – можливо;
– низька (Low Probability) – малоймовірно.

Для збитку (Impact – міра величини втрат або шкоди, що завдається активу):

– «В» (High Impact) – зупинка критично важливих бізнес-підрозділів, яка призводить до істотного збитку для бізнесу, втрати іміджу або неотримання істотного прибутку;

– «С» (Medium Impact) – короткочасне переривання роботи критичних процесів або систем, що призводить до обмежених фінансових втрат в одному бізнес-підрозділі;

– «Н» (Low Impact) – перерва в роботі, що не викликає відчутних фінансових втрат.

Оцінка здійснюється у відповідності з правилом, яке задається матрицею ризиків (рис. 3.22) і може інтерпретуватися наступним чином:

– рівень А – пов'язані з ризиком заходи (наприклад, впровадження засобів ЗІ) повинні бути виконані негайно і в обов'язковому порядку;

– рівень В – пов'язані з ризиком заходи мають бути вжиті;

– рівень С – потрібний моніторинг ситуації (але безпосередніх заходів з протидії загрозі приймати, можливо, не треба);

– рівень D – ніяких заходів в даний момент робити не треба [41].

PROBABILITY / **IMPACT**

	High	Medium	Low
High	*A*	*B*	*C*
Medium	*B*	*B*	*C*
Low	*B*	*C*	*D*

A – Corrective action must be implemented
B – Corrective action should be implemented
C – Requires monitor
D – No action required at this time

Рис. 3.22. Матриця ризиків FRAP

Етап 4 – Визначення контрзаходів. Після ідентифікації загроз та ОР визначаються контрзаходи, які дозволяють усунути ризик або звести його до прийнятного рівня.

Етап 5 – Документування. Після АОР результати детально документуються в стандартизованому форматі. Отриманий звіт може бути використаний для визначення політик, процедур, бюджету ІБ тощо.

Методика Risk Matrix

Методика Risk Matrix [42] (розробник компанія Mitre Corporation, США) орієнтована на АОР і згодом була реалізована додатком для Microsoft Excel. Основний процес включає: планування оцінювання ступеня ризику; ідентифікацію завдань або вимог; визначення; ранжування; складання рейтингу ризиків; управління планами дій; безперервну оцінку ризиків.

Оцінювання ризику полягає в плануванні діяльності. Спочатку проводиться ідентифікація ризику за допомогою застосування експертами «Мозкового штурму».

Далі присвоюються різні атрибути кожному ризику, такі як, наприклад, період часу (дати початку і закінчення можливої реалізації) та ЙВ.

За допомогою сценарію «Якщо ризик ..., то наслідки ...» складається матриця ризику.

Для визначення впливів використовується шкала:

- C (критичні);
- S (серйозні);
- M_o (середні);
- M_i (низькі);
- N (незначні).

A для ймовірності – (P):

- 0-10% (дуже низька);
- 11-40% (низька);
- 41-60% (середня);
- 61-90% (вище середнього);
- 91-100% (висока).

На етапі ранжування використовується метод Borda і далі складається рейтинг ризику з визначенням його ступеня – «H», «C» або «B» табл. 3.32 [42]. Для визначення найбільш пріоритетних ризиків використовується діаграма частот (рис. 3.23). Приклад матриці ризику представлений на рис. 3.24 [42].

ternational Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

20) Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности», BS ISO/IEC 27005:2011, К.: 2011, с. 94.

21) «Expression des Besoins et Identification des Objectifs de Sécurité EBIOS», Méthode de gestion des risques, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

22) C. Harpes, A. Adelsbach, S. Zatti, N. Peccia, «Quantitative Risk Assessment with ISAMM on ESA's Operations Data System», Itrust consulting, 2007. [Online]. Available: https://www.itrust.lu/ wp-content/uploads/ 2007/ 09/publications_ TTC_ 2007_abstract_ risk_ assessment_with_ISAMM.pdf. [Accessed: 19- Jan- 2017].

23) «IRAM2 Managing information risk is a business essential», Information Security Forum Limited, 2017. [Online]. Available: https://www.securityforum.org/ upl-oads/2015/03/ISF-IRAM2-ES.pdf. [Accessed: 20- Jan- 2017].

24) «Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models», COBIT 4.1., Rolling Meadows: IT Governance Institute, 2007, p. 196.

25) В. Олифер, Н. Олифер, Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов, [3-е изд.], СПб: Питер, 2006, с. 958.

26) С. Нестеров, Анализ и управление рисками в информационных системах на базе операционных систем Microsoft, [Учебный курс.], Санкт-Петербург: Издательство «INTUIT», 2009, с. 136.

27) С. Петренко, С. Симонов, Управление информационными рисками. Экономически оправданная безопасность, М.: Компания АйТи, ДМК Пресс, 2004, с. 384.

28) «Practical Threat Analysis in-depth», PTA Technologies, 2013. [Online]. Available: http://www.ptatechnologies.com/ default.htm. [Accessed: 20- Jan- 2017].

29) Д. Костров, «Анализ рисков и управление ими», Byte Россия, №10 (62), С. 15–20, 2003.

30) С. Симонов, «Анализ рисков в информационных систе-мах. Практические аспекты. Защита информации», Конфидент. Безопасность компьютерных систем, №2, С. 48-53, 2001.

11) С. Казмірчук, В. Волянська, «Дослідження методик оцінки ризиків», Сучасні проблеми захисту інформації з обмеженим доступом: міжвідомча науково-практ. конф., тези доп., К., 2008, С. 67–69.

12) И. Медведовский, «Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ» [Электронный ресурс], SecurityLab, Мн.: SecurityLab, 2004, [Online]. Режим доступа: http://www.ixbt.com/cm/informationsystem-risks012004.shtml. [просмотрено 18 декабря 2011].

13) А. Алексеев «Управление рисками. Метод CRAMM», IT Expert, М.: ЗАО «ИТ Эксперт», 2010. [Online]. Режим доступа: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. [просмотрено 19 декабря 2010].

14) О. Потій, А. Лєншин, «Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу», Збірник наукових праць Харківського університету Повітряних Сил, № 2(24), С. 85–91, 2010.

15) А. Частиков, И. Леднева, «Использование байесовской сети при разработке экспертных систем с нечеткими знаниями», [Электронный ресурс], Краснодар Кубанский государственный технологический университет, 2005, [Online]. Режим доступа: http://ito.su/2000/II/5/5152.html.

16) Jeevan Jaising, Jackie Rees Krannert, «Value at Risk: A methodology for Information Security Risk Assessment», Proceedings of The 6th INFORMS Conference on Information Systems and Technology (CIST-2001), Miami Beach, Florida, November 2001, p. 15.

17) «Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA» [Electronic resource], Security Risk Analysis & Assessment, and ISO 27000 Compliance, Macclesfield: The Leading Security Risk, 2010, [Online]. Access mode: http://www.riskworld.net/.

18) Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen, «Model-Driven Risk Analysis. Chapter: A Guided Tour of the CORAS Method», 2011, SINTEF ICT, Oslo, Norway, pp 23-43.

19) «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, In-

Таблиця 3.32. Шкала ризику

ПЙР (%)	Категорії дії				
	N	M_i	M_o	S	C
0-10	H	H	H	C	C
11-40	H	H	C	C	B
41-60	H	C	C	C	B
61-90	C	C	C	C	B
91-100	C	B	B	B	B

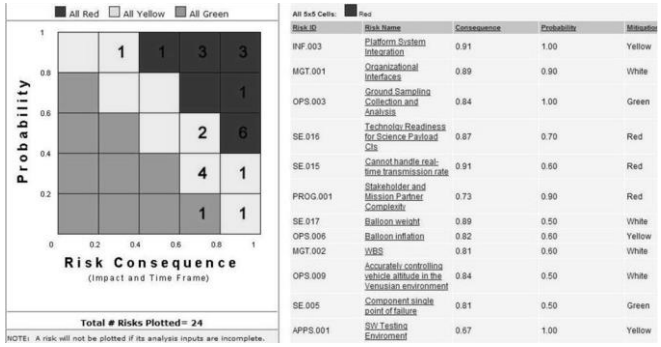


Рис. 3.23. Діаграма частот

	A	B	F	G	H	J	K	O	P	U
1	Risk No.	Related Risk	RISK	Timeframe Start	Timeframe End	I	Po (%)	Borda Rank	R	Manage/Mitigate
2	1	4	IF contract is not awarded before 30 Sep, THEN program loses $8M in expiring funds.	30 Jan 1999	30 Sep 1999	C	60%	0	H	Use existing Task Order contract to assure award before 30 Sep.
3	2	N/A	IF unmodified commercial laptops are used, THEN operational availability cannot be met in intended environment.	28 Feb 1999	28 Feb 2000	S	100%	0	H	Limit buy for first release and plan technology insertion for improved environmental performance for second release.
4	3	4	IF DII COE V1.5 is more than 1 mo. late, THEN first release will slip day for day.	30 Jan 1999	30 Oct 1999	S	90%	3	M	Use DII COE V1.4 for first release and modify requirements.
5	4	1,3	IF first release is not demonstrated in EFX, THEN program will be assigned to Navy.	15 Feb 1999	15 Apr 2000	C	60%	0	H	Integrate only those capabilities available at contract award for first release.
6	5	1	IF all KPPs must be satisfied by second release, THEN program funding is insufficient.	30 Jan 1999	30 Jul 2001	S	40%	4	M	Use CAIV to prioritize release content subject to budget and plan for third and fourth release.

RiskEntries / ChartI / ChartPo

Рис. 3.24. Приклад матриці ризику

Методика Mehari

Методика Mehari (називають методологією) [43] (розробник Clusif, Франція) замінила систему Clarion і є структурованим під-

ходом до ОР. Вона дає можливість ЯК і КЛ оцінити чинники ризику та РР. При цьому, Mehari інтегрує інструменти (наприклад, критерії оцінки, формули та ін.) і бази знань (зокрема, заходи для діагностики ІБ), що є важливим доповненням до мінімальних методів запропонованих в ISO/IEC 27005.

Для того, щоб відповісти на питання «Які ризики є високими для організації та прийнятні вони чи ні?» застосовується структурований підхід для виявлення всіх можливих подій ризику, аналіз індивідуально найбільш важливі з них, а потім визначити дії щодо зниження ризику до прийнятного рівня.

Для оцінки пропонуються два основні варіанти – використання баз знань (які інтегруються в Microsoft Excel, Open Office) або ПЗ (наприклад, Risicare, яке забезпечує більш багатий користувальницький інтерфейс, а також дозволяє моделювати, візуалізувати та оптимізувати отримані результати).

Для оцінки використовується структурована модель ризику, яка враховує «чинники зниження ризику» [44]. Процес АОР реалізується в 9 етапів:

1. Ідентифікація ризику. Пропонуються два підходи – прямий (передбачає ідентифікацію несправностей або подій, які можуть призвести до порушення ІБ, в результаті будуть описані можливі типи несправностей) та системний (полягає у використанні великих баз знань для ведення автоматизованої оцінки).

2. Оцінка впливу. Тут використовується ЯК шкала, де:

– 1 – дуже низька експозиція (незалежно від будь-яких заходів ІБ, ймовірність того, що такий сценарій буде відбуватися – дуже низька);

– 2 – низький вплив (ймовірність того, що такий сценарій відбудеться в короткостроковий або середньостроковий період – низька);

– 3 – середня експозиція (якщо нічого не робити, то такий сценарій повинен відбутися в більш-менш короткий термін);

– 4 – високий рівень впливу (якщо нічого не буде зроблено, то такий сценарій неминучий в дуже короткий термін).

3. Оцінка стримуючих чинників. Проводиться аудит стримуючих та профілактичних чинників, які можуть запобігти виникненню ризику.

СПИСОК ЛІТЕРАТУРИ ДО ТРЕТЬОГО РОЗДІЛУ

1) «Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]», National Institute of Standards and Technology Special Publication 800-30, Falls Church: Natl. Inst. Stand. Technol, 2002, p. 54.

2) «Risk analysis based on IT-Grundschutz», BSI-Standard 100-3, Boon: Bundesamt für Sicherheit in der Informationstechnik, 2008, p. 23.

3) «Рекомендации в области стандартизации банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности», [Электронный ресурс], РС БР ИББС-2.2-2009, Введ. 2010.01.01, Банк России: Официальный сайт, М.: Банк России. [Online]. Режим доступа: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. [просмотрено 29 декабря 2011].

4) «Information Technology – Security techniques – Information security risk management (ISO/IEC 27005:2008)», ISO/IEC JTC 1/SC 27, 2008, p. 62.

5) «Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности», BS ISO/IEC 27005:2008, К.: 2011, с. 70.

6) М. Луцкий, Е. Иванченко, А. Корченко, С. Казмирчук, А. Охрименко, «Современные средства управления информационными рисками», Захист інформації, №1, С. 5–16, 2012.

7) А. Корченко, А. Архипов, С. Казмирчук, Анализ и оценивание рисков информационной безопасности. Монография, Киев: ООО «Лазурит-Полиграф», 2013, с. 275.

8) «Risk management», Standard AS/NZS 4360:2004, Nundah : ISO working group – risk management Terminology, 2004, p. 65.

9) «International standard Risk management. Principles and guidelines», ISO/FDIS 31000:2009(E), International Organization for Standardization, JISC, 2009, p. 24.

10) В. Галатенко, Стандарты информационной безопасно-сти, М.: Интернет-Университет Информационных технологий, 2004, с. 328.

прокоментувати ризики і включити обґрунтування для вирішення, що перевищує стандартний критерій прийняття ризиків [20].

Наказ вищого керівництва про прийняття остаточних ризиків.

Вище керівництво приймає такі ризики
Ризик 1 - Величина 10 - Причина 1
Ризик 2 - Величина 17 - Причина 2
Ризик 3 - Величина 3 - Причина 3
Генеральний директор …
Дата Підпис

Питання для самоконтролю

1) Що таке ризик?
2) Які стандарти регламентують процес ризик-менеджменту?
3) Що собою являє процес аналізу ризику?
4) Що таке оцінка ризиків?
5) Які процеси складають оцінку ризику?
6) Наведіть кількісні методи оцінювання ризиків?
7) Наведіть якісні методи оцінювання ризиків?
8) Які ви знаєте відкриті бази даних уразливостей?
9) Що собою являє оцінка CVSS?
10) Що таке актив для підприємства?
11) Опишіть процес ідентифікації активів
12) Що таке контрольні заходи?
13) Які процеси відображають обробку ризику?
14) Опишіть процес прийняття ризику?
15) Які дії відображають ризик-менеджмент?

4. Оцінка захисних, паліативних та рекуперативних чинників.

5. Оцінка потенційності. Оцінюються потенційні ризики (які повинні відбутися) на підставі п'ятибальної шкали:

– 0 – відсутня;
– 1 – дуже малоймовірно;
– 2 – малоймовірно;
– 3 – швидше за все;
– 4 – дуже ймовірно.

6. Оцінка впливу. Проводяться оцінки наслідків настання ризику незалежно від будь-яких заходів ІБ.

7. Оцінка впливу після вжиття заходів щодо зниження ризику та показників скорочень впливу.

8. Глобальна ОР. Визначаються глобальні ризики для організації.

9. Прийняття рішення про прийнятність або неприйнятність ризику [43].

Методика MAGERIT

Методика MAGERIT [45] (Methodology for Information Systems Risk Analysis and Management, розробник Ministerio De Administraciones Públicas, Іспанія) призначена для реалізації процесу АОР, який здійснюється в 3 етапи:

Етап 0 – Планування.

Етап 1 – Аналіз ризику. Складається з 5 кроків:

1. Ідентифікація та оцінка активів, які є елементами ІС (або тісно пов'язаних з нею), цінними для організації. Активи пропонується розділяти на 5 груп (навколишнє середовище, ІС, інформація, функції організації, інші активи) для визначення залежності між ними. Після ранжування активів проводиться їх оцінка щодо вартості. Далі визначаються вимоги до К, Ц і Д та автентичності активу;

2. Аналіз і ОЗ ІБ. За допомогою категорії загроз, яка наведена в даній методиці, проводиться їх ідентифікація, реалізується оцінка частоти (використовується шкала: 100 – дуже часто (щодня); 10 – часто (щомісяця); 1 – зазвичай (щорічно); 1/10 – рідко (раз в декілька років)) та збитків;

3. Визначення превентивних заходів для запобігання загрози;

4. Оцінка впливу. Вимірювання пошкодження активів, пов'язаних з загрозою;

5. Визначення ризику. Ризик відображається ймовірністю пошкодження ІС та збільшується зі зростанням впливу і частоти (табл. 3.33 [45]).

Етап 2 – Управління ризиками. Вибираються та реалізуються захисні заходи (технічні, фізичні [46], організаційні, робочого середовища для людей і устаткування та кадрова політика), а також здійснюється інтерпретація значення для впливу і залишкових ризиків, проводиться аналіз прибутку та збитків [45].

Таблиця 3.33. Приклад потенційних загроз файлам даних

		Вимірювання ІБ (%)						
актив/загроза	**F**	**D**	**I**	**C**	**AS**	**AD**	**TS**	**TD**
[D_exp] Поточні файли		**50**	**50**	**100**	**100**	**100**	**100**	**100**
[E.1] Помилки користувачів	10	10	10					
[E.2] Помилки адміністратора	1	20	20	10	10	10	20	20
[E.3] Помилки моніторингу	1						50	50
[E.4] Помилки конфігурації	0,5	50	10	10	50	50	50	50
[A.4] Зміни конфігурації	0,1	50	10	50	100	100	100	100
[A.11] Несанкціонований доступ	100		10	50	50			

Приклади оцінок показані в ПЗ «Techniques Guide» на рис. 3.25 а-б, де:

- D, I та C – відповідно К, Ц та Д даних;
- AS і AD – відповідно справжність користувача послуг та походження даних;
- TS і TD – відповідно підзвітність використання послуг і доступу до даних [45, 47].

Методика Information Security RA

Методика Information Security RA [48] (Risk Assessment, розробник Centers for Medicare & Medicaid Services (CMS), США) надає можливість реалізації АОР у сфері ІБ. Методика складається з 3 фаз:

Фаза 1. Документування системи. Фаза реалізується декількома процесами – ідентифікація системної документації та активів, а також визначення поточного рівня ІБ (з використанням шкали: «В», «С» та «Н», табл. 3.34 [48]);

Фаза 2. Визначення ризику. Розрахунок РР для кожної пари загрози і уразливості, на основі ймовірності того, що загроза з використанням уразливості буде здійснена. Також визначається ступінь

Перенесення ризику

Перенесення ризику включає в себе рішення розділити певні ризики з зовнішніми сторонами. Перенесення ризику може створювати нові ризики або модифікувати існуючі ідентифіковані ризики. Тому може бути необхідна додаткова обробка ризику.

Перенесення може бути здійснене страхуванням, яке буде підтримувати наслідки, або за допомогою укладення договору субпідряду з «партнером», чия роль буде полягати у проведенні моніторингу ІС і здійсненні негайних дій з припинення атаки, перш ніж вона приведе до певного рівня шкоди.

Слід зауважити, що може бути можливим перенести відповідальність, пов’язану з менеджментом ризику, але, зазвичай, неможливо перенести відповідальність за шкоду. Клієнти зазвичай приймають несприятливий вплив збитку, як помилку організації [20].

3.6. Прийняття ризику інформаційної безпеки

У планах обробки ризику повинно описуватися те, як оцінювати ризики, які слід обробляти для того, аби відповідати критеріям прийняття ризиків.

Важливо, щоб відповідальні менеджери переглядали і підтримували пропоновані плани обробки ризику і витікаючі з них залишкові ризики, а також реєстрували всі умови, пов’язані з підтримкою прийнятих рішень.

Критерії прийняття ризику можуть бути більш багатогранним аспектом, ніж просто визначення того, чи знаходиться залишковий ризик вище або нижче єдиного порогового значення.

У деяких випадках рівень залишкового ризику може не відповідати критеріям прийняття ризику, оскільки застосовувані критерії не враховують переважаючі обставини. Наприклад, може бути доведено, що необхідно приймати ризики через вигоди, пов’язані з ризиками, які можуть бути дуже привабливими, чи тому що витрати, пов’язані з зниженням ризику, дуже високі. Такі обставини показують, що критерії прийняття ризику є неадекватними і повинні бути по можливості переглянуті. Однак, не завжди можливо передивитись критерії прийняття ризику своєчасно. У таких випадках особи, які приймають рішення можуть бути зобов’язані прийняти ризики, які не відповідають стандартним критеріям прийняття. Якщо це необхідно, особа, яка приймає рішення, має явним чином

користувачами). Більш того, може статися так, що засоби контролю будуть впливати на продуктивність. Менеджери повинні працювати над ідентифікацією рішення, яке задовольняє вимогам продуктивності, в той же час гарантує достатню ІБ. Результатом цього першого кроку є перелік можливих засобів контролю з їх вартістю, вигодою і пріоритетом реалізації.

При формуванні рекомендацій і в процесі реалізації повинні прийматися в розрахунок різні обмеження. Типовими обмеженнями є:

- тимчасові обмеження;
- фінансові обмеження;
- технічні обмеження;
- операційні обмеження;
- культурні обмеження;
- етичні обмеження;
- обмеження, пов'язані з навколишнім середовищем;
- юридичні обмеження;
- простота використання;
- кадрові обмеження;
- обмеження, що стосуються інтеграції нових та існуючих засобів контролю.

Збереження ризику

Якщо рівень ризику відповідає критеріям прийняття ризику, то немає необхідності реалізовувати додаткові засоби контролю і ризик може бути збережений.

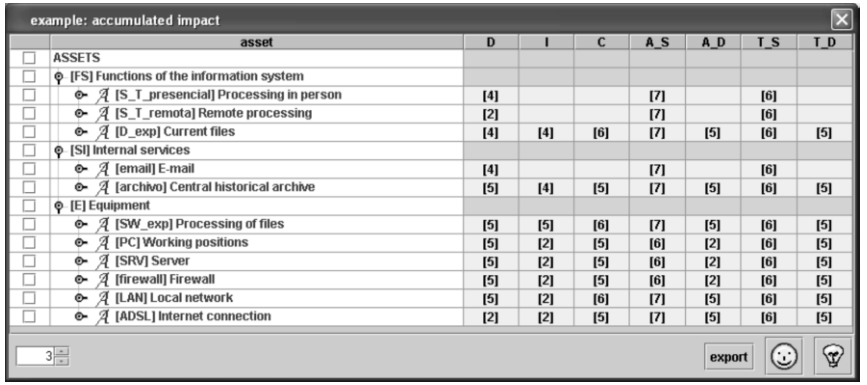
Запобігання ризику

Коли ідентифіковані ризики вважаються занадто високими або витрати на реалізацію інших варіантів обробки ризику перевищують вигоду, може бути прийнято рішення про повне запобігання ризику шляхом припинення програми або відмови від запланованої чи існуючої діяльності, або сукупності дій чи Зміни умов, при яких проводиться діяльність (дії) . Наприклад, щодо ризиків, що викликаються природними факторами, найбільш економічно вигідною альтернативою може бути фізичне переміщення засобів обробки інформації туди, де цей ризик не існує або перебуває під контролем.

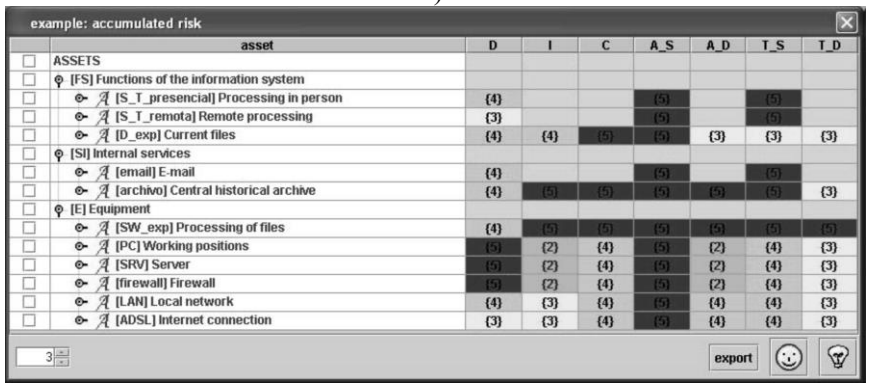
впливу, який загроза матиме на ІС (її дані і бізнес-функції) з точки зору втрати К, Ц і Д.

Фаза 2 складається з 6 кроків:

1. Виявлення загрози;
2. Визначення уразливості;
3. Виявлення існуючих елементів управління для зниження ризику реалізації даної загрози (з використання уразливості).



а)



б)

Рис. 3.25. Приклад оцінки: а) впливу; б) ризику

4. Визначення її ймовірності виникнення з урахуванням наявних елементів управління, для чого використовується семирівнева шкала:

- НЗ – незначна (малоймовірно);

– ДН – дуже низька (ймовірно два/три рази в п'ять років);
– Н – низька (відбудеться один раз на рік або менше);
– С – середня (може статися один раз в шість місяців або менше);
– В – висока (відбудеться один раз на місяць або менше);
– ДВ – дуже висока ймовірність (кілька разів на місяць);
– ЕЙ – екстремально ймовірно (кілька разів на день).

Таблиця 3.34. Рівні ризику

ЙВ	Вплив					
	НЗ	МЛ	ЗН	ПШ	СЗ	КР
НЗ	Н	Н	Н	Н	Н	Н
ДН	Н	Н	Н	Н	С	С
НК	Н	Н	С	С	В	В
СР	Н	Н	С	В	В	В
ВС	Н	С	В	В	В	В
ДВ	Н	С	В	В	В	В
ЕЙ	Н	С	В	В	В	В

5. Оцінювання ступенів впливу на систему здійснюється за шестирівневою шкалою:
– НЗ – незначний;
– МЛ – малий;
– ЗН – значний;
– ПШ – пошкоджуваний;
– СЗ – серйозний;
– КР – критичний.

6. Визначення РР для даної пари загроза – уразливість наявних елементів управління. РР визначаються згідно табл. 3.34 [6, 7, 11, 48-50].

3.3. Сучасні бази даних уразливостей інформаційної безпеки

При побудові різних систем ЗІ (наприклад, СМІБ [19]) виникає необхідність здійснювати оцінювання стану ІБ з урахуванням відомих уразливостей РІС. Тому, перед фахівцями, які займаються дослідженням стану безпеки ІС, виникає питання про ефективність використання відповідних БД уразливостей, які відповідають певним критеріям [51-55], таким, наприклад, як наявність ідентифіка-

Після того як був визначений план обробки ризику, необхідно визначити залишкові ризики. Це включає оновлення або повторну операцію оцінки ризику, беручи до уваги очікуваний ефект від передбачуваної обробки ризику. Якщо залишкові ризики як і раніше не будуть задовольняти критеріям прийняття ризику організації, може виникнути необхідність подальшої ітерації обробки ризику, перш ніж перейти до прийняття ризику.

Зниження ризику

Повинні бути вибрані відповідні і обґрунтовані засоби контролю для того, щоб задовольняти вимогам, ідентифікованим за допомогою оцінки ризику і процесу обробки ризику. Такий вибір повинен враховувати критерії прийняття ризиків, а також правові, регулюючі та договірні вимоги. Цей вибір повинен також взяти до уваги вартість і період реалізації засобів контролю або технічні аспекти, аспекти середовища або культурні аспекти. Найчастіше можна знизити загальні витрати власника системи за допомогою відповідним чином обраних засобів контролю безпеки.

В цілому, засоби контролю можуть забезпечувати один або декілька з наступних видів захисту: виправлення, виключення, попередження, зменшення впливу, стримування, виявлення, відновлення, моніторинг та інформованість. Під час вибору засобів контролю важливо «зважувати» вартість придбання, реалізації, адміністрування, функціонування, моніторингу та підтримки засобів контролю по відношенню до цінності активів, які захищаються. Крім того, рентабельність інвестицій з точки зору зниження ризику, і потенціал для використання нових можливостей бізнесу, що надаються певними засобами контролю. Додатково слід звернути увагу на спеціалізовані навички, які можуть знадобитися для визначення та реалізації нових засобів контролю або модифікації існуючих.

Існує багато обмежень, які можуть впливати на вибір засобів контролю. Технічні обмеження, такі як вимоги до функціонування, питання керованості (вимоги операційної підтримки) і сумісності можуть перешкоджати використанню певних засобів контролю або можуть вводити помилку персоналу, також можуть анулювати засоби контролю, вселяючи помилкове відчуття безпеки, чи навіть збільшувати ризик, по відношенню до того як якби не було ніякого засобу контролю (наприклад, вимоги використання складних паролів без відповідного навчання, що може привести до запису паролів

клад, засоби контролю безперервності бізнесу, які розглядаються для охоплення специфічних високих ризиків).

Чотири варіанти обробки ризиків не є взаємовиключними. Іноді організація може значно виграти від об'єднання варіантів, таких як зниження ймовірності ризику, Зменшення їх наслідків і перенесення або збереження будь-яких залишкових ризиків.

Деякі види обробки ризиків можуть бути ефективними для більш ніж одного ризику (наприклад, навчання та обізнаність в частині ІБ). План обробки ризику повинен чітко визначати порядок пріоритетів, в якому повинна реалізовуватися обробка окремих ризиків. Порядок пріоритетів може встановлюватися з використанням різних методів, включаючи ранжування ризиків і аналіз «витрати-вигода». В обов'язки керівництва входить прийняття рішення про баланс між витратами на реалізацію засобів контролю та бюджетними відрахуваннями.

Ідентифікація існуючих засобів контролю може визначати ті існуючі засоби контролю, які перевищують поточну потребу також і з точки зору порівняння витрат, включаючи підтримку. Якщо розглядається видалення надлишкових або непотрібних засобів контролю (особливо, якщо витрати на підтримку цих засобів контролю великі), повинні прийматися до уваги чинники ІБ і вартості. Оскільки засоби контролю впливають один на одного, видалення надлишкових засобів контролю може в підсумку знизити ефективність використання всіх засобів забезпечення безпеки, які залишилися. Крім того, може бути дешевше залишити надлишкові або непотрібні засоби контролю, ніж видалити їх.

Варіанти обробки ризику повинні враховувати:

– як ризик усвідомлюється ураженими сторонами;
– найбільш відповідні шляхи комунікації з цими сторонами.

Встановлення контексту дає інформацію про правові і регулюючі вимоги, яким необхідно слідувати організації. Для організацій є ризиком відмова від відповідності зазначеним вимогам, у зв'язку з цим мають бути розглянуті варіанти обробки для обмеження цієї можливості. Всі обмеження – організаційні, технічні, структурні та інші, які повинні бути визначені протягом діяльності, пов'язаної з встановленням контексту, слід брати до уваги протягом обробки ризику.

торів CVE, оцінок CVSS, CWE категорій, CVSS-калькулятора, ризик-калькулятора тощо. Використання зазначених критеріїв дозволить здійснити раціональний вибір таких БД. У зв'язку з цим, актуальною є задача дослідження відповідних БД для визначення набору критеріїв, згідно яких можна ефективно використовувати такі бази.

На сьогодні існує широка множина загальнодоступних БД уразливостей PIC, які піддавалися аналізу в різних джерелах. Так, в роботі [53] проводилося дослідження відкритих БД уразливостей, де авторами були визначені основні поля записів уразливостей, переваги та недоліки розглянутих баз, але не визначені узагальнені критерії, за якими можна здійснювати такий аналіз. Також в роботах [54, 56] розглянуті БД з точки зору наявності посилань на інші бази, можливості отримання інформації в форматі XML, а також форматі представлення уразливостей в БД. Слід зазначити, що в [54, 56] не визначені чіткі критерії, за якими можна здійснити відповідний аналіз. Авторами роботи [55] при обгрунтуванні вибору БД за основу були прийняті наступні критерії:

− повнота (ємність, кількість уразливостей);
− доступність даних (безкоштовна база);
− зручність отримання даних (інтерфейси);
− підтримка оцінки уразливостей за системою CVSS, але здебільшого робився акцент на уразливості, які впливають на доступність.

Також слід зазначити, що в роботах [51-56] не були чітко виділені критерії, за якими можна порівняти БД уразливостей і здійснити їх вибір для побудови різних систем оцінювання в області ІБ, наприклад, таких як системи АОР.

У зв'язку з цим, проведемо дослідження широкого спектру існуючих БД уразливостей для визначення критеріїв, за якими можна здійснити порівняльний аналіз вищезгаданих баз і використовувати їх при АОР ІБ.

Для проведення такого дослідження скористаємося найбільш відомими і загальнодоступними БД уразливостей:

– національна БД уразливостей – National Vulnerability Database (NVD), (США) [57];

– банк даних загроз безпеки інформації (Російська Федерація) [58];

– відкрита БД уразливостей – Open Sourced Vulnerability Database (OSVDB), (США) [59];

– БД уразливостей IBM X-Force, (США) [60];

– БД записів уразливостей US-CERT – Vulnerability Notes Database US-CERT (VND), (США) [61];

– БД уразливостей SecurityFocus, (США) [62].

Розглянемо кожну з них.

National Vulnerability Database

База National Vulnerability Database розроблена National Institute of Standards and Technology (NIST) Computer Security Division, Information Technology Laboratory за підтримки Department of Homeland Security's National Cyber Security Division. Вона є державним сховищем даних США, яке засноване на стандартах управління уразливостями. Такі дані дозволяють автоматизувати процеси управління уразливостями, вимірювати стан ІБ і визначати його відповідність. База NVD включає в себе БД контрольних списків безпеки, недоліків PIC, неправильних конфігурацій, PIC і показників впливу.

БД є репозитарієм основних стандартів управління даними уразливостей, розроблений на основі протоколу автоматизації контенту безпеки – Security Content Automation Protocol (SCAP) [57].

Існують наступні компоненти SCAP:

– БД уразливостей безпеки – Common Vulnerabilities and Exposures (CVE);

– БД уразливих конфігурацій PIC – Common Configuration Enumeration (CCE);

– стандартна номенклатура та база імен PIC – Common Platform Enumeration (CPE);

– БД слабких місць – Common Weakness Enumeration (CWE);

– стандарт оцінки впливу уразливостей – Common Vulnerability Scoring System (CVSS);

– стандарт XML-специфікації контрольних листів – Extensible Configuration Checklist Description Format (XCCDF);

– стандарт XML-специфікації контролю станів процесів – Open Vulnerability and Assessment Language (OVAL) [57].

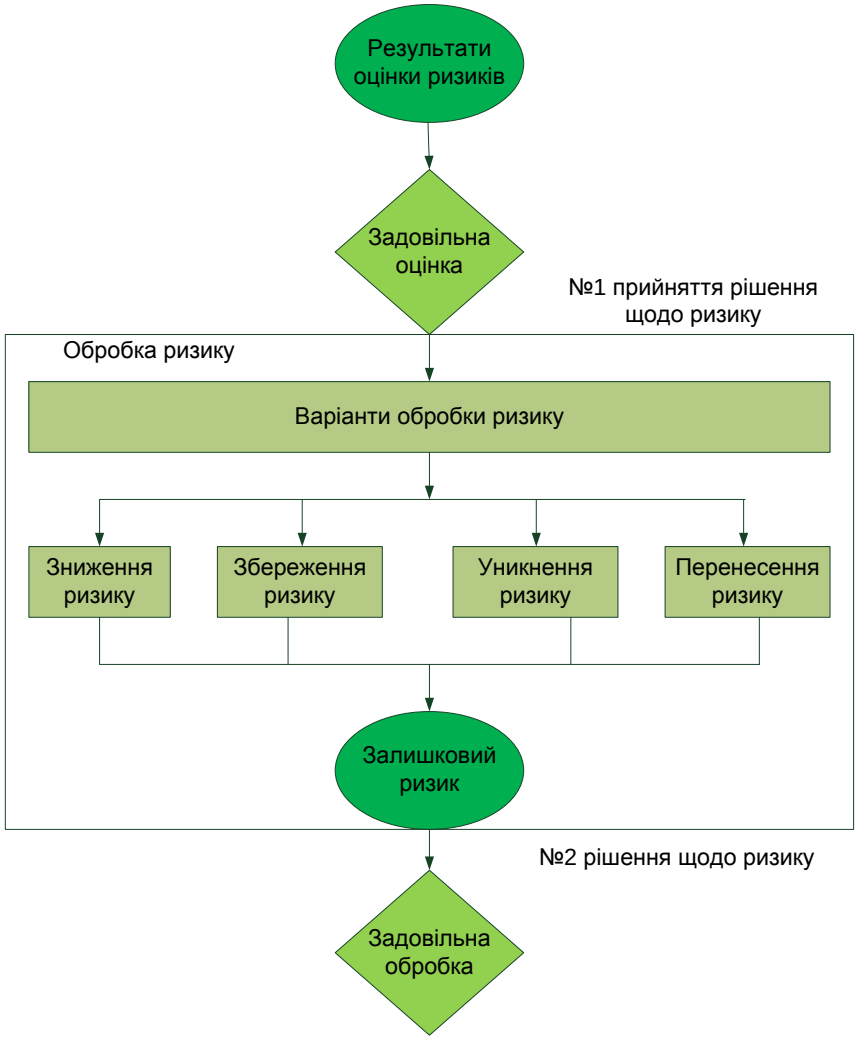


Рис. 3.50. Діяльність обробки ризику

Несприятливі наслідки ризиків необхідно знижувати до розумних меж і незалежно від будь-яких абсолютних критеріїв. Менеджери повинні розглядати рідкісні, але серйозні ризики. У таких випадках може виникнути необхідність реалізації засобів контролю, які є не обгрунтованими із суто економічних причин (напри-

3.5. Обробка ризиків інформаційної безпеки

Організація повинна визначити та застосовувати процес оброблення ризиків ІБ для:

а) вибору доречних опцій оброблення ІБ з урахуванням результатів оцінки ризиків;

б) визначити всі заходи безпеки, які необхідно впровадити для вибраної(-их) опції(-ій) оброблення ризиків;

в) порівняти заходи безпеки, визначені в п. 3.4 б) вище, і підтвердити, що не було опущено потрібних заходів безпеки;

г) підготувати Положення щодо застосовності, яке містить:

– необхідні заходи безпеки;
– обґрунтування для їх застосування;
– впроваджені необхідні заходи безпеки чи ні;
– обґрунтування для виключень заходів безпеки;

д) розробити план оброблення ризиків ІБ;

е) отримати від власників ризиків підтвердження плану оброблення ризиків ІБ та згоду на залишкові ризики ІБ.

Організація повинна зберігати задокументовану інформацію щодо процесу оброблення ризиків ІБ [68].

Визначення та оцінка варіантів обробки ризиків

Що можна зробити з існуючими ризиками?

1) Застосування відповідних коштів;

2) Розумне і цільове прийняття ризиків, що забезпечує їх повне задоволення політикою організації та її критеріям прийняття ризиків;

3) Уникнення ризиків;

4) Перенесення пов'язаних бізнес-ризиків на інші сторони, наприклад на страховиків, постачальників та ін.

На рис. 3.50 ілюструється діяльність з обробки ризику в рамках процесу менеджменту ризику ІБ.

Варіанти обробки ризику повинні обиратися на основі результатів оцінки ризику, очікуваної вартості реалізації цих варіантів і очікуваної вигоди від цих варіантів.

Коли значне зниження ризику може бути досягнуто при відносно невеликих витратах, такі варіанти повинні реалізовуватися. Додаткові варіанти поліпшень можуть бути неекономічними, і рішення необхідно вивчати у відношенні того, чи є вони виправданими.

Крім цього застосовується наступний набір інших протоколів.

Threat Analysis Automation Protocol (TAAP) – протокол документування та спільного використання структурної інформації про загрози. Він містить такі компоненти:

– БД атрибутів шкідливого ПЗ – Malware Attribute Enumeration & Characterization (MAEC);
– БД шаблонів атак – Common Attack Pattern Enumeration & Classification (CAPEC);
– CPE;
– CWE;
– OVAL;
– CCE;
– CVE.

Event Management Automation Protocol (EMAP) – протокол для звітів про події безпеки. Він має такі складові:

– БД записів подій – Event Expression (CEE);
– MAEC;
– CAPEC.

Incident Tracking and Assessment Protocol (ITAP) – протокол для відстеження, документування, управління та спільного використання інформації про інциденти. Він містить наступні компоненти:

– OVAL;
– CPE;
– CCE;
– CVE;
– CVSS;
– MAEC;
– CAPEC;
– CWE;
– CEE;
– формат обміну описом інциденту – Incident Object Description Exchange Format (IODEF);
– національна модель обміну інформацією – National Information Exchange Model (NIEM);
– формат обміну інформацією з кібербезпеки – Cybersecurity Information Exchange Format (CYBEX) [57].

Розглянуті протоколи, стандарти і БД NVD на практиці, наприклад, можна використовувати в наступних цілях:

CPE – визначення ІС підприємства;

CVE – ідентифікація уразливостей;

CVSS – визначення критичних уразливостей;

CCE – формування найбільш захищеної конфігурації ІС;

XCCDF – визначення політики захищеної конфігурації;

OVAL – оцінка відповідності системи політиці захищеної конфігурації;

CWE – визначення слабких місць РІС;

CAPEC – визначення атак відносно слабких місць РІС;

CEE – визначення подій для реєстрації та параметрів реєстрації;

ARF – об'єднання результатів оцінки;

MAEC – визначення шкідливого ПЗ.

Слід зазначити, що в NVD обчислюється індекс робочого навантаження на інформацію I_W, який показує кількість критичних уразливостей. Чим вище число, тим більше навантаження на систему безпеки. Індекс навантаження NVD розраховується за формулою

$$I_W = (N_h + (N_m / 5) + (N_l / 20)) / 30,$$

де N_h, N_m та N_l – кількість уразливостей з високим, середнім і низьким ступенем тяжкості відповідно, які були опубліковані протягом останніх 30 днів. Як видно з формули, одна уразливість високого ступеня тяжкості прирівнюється до п'яти уразливостей із середнім і двадцяти з низьким ступенем тяжкості [57]. На сайті NVD доступний повний список уразливостей, які містяться в базі та упорядковані за роками та місяцями (див. рис. 3.26).

Кожна уразливість, яка вноситься в БД, описується наступними параметрами (рис. 3.27):

- унікальний CVE-ідентифікатор;
- дата внесення в БД;
- дата останньої редакції;
- джерело уразливості (інформації);
- короткий опис (огляд);
- результати оцінок з кожної метричної групи (МГ) CVSS (див. рис. 3.27, 3.28 і табл. 3.35) – базової (Base Score), часової (Temporal

Таблиця 3.43. Приклад шкали для ранжирування і розрахунку ризику

Імовірність / Збитки	Дуже низька	Низька	Середня	Висока	Дуже висока
Низький	1	3	5	7	9
Середній	3	9	15	21	27
Високий	5	15	25	35	45
Дуже високий	7	21	35	49	63

Звіт про аналіз ризиків (див. табл. 3.44)

Таблиця 3.44. Приклад звіту про аналіз ризику

Місцезнаходження	**Категорія (Код активу)**	**Актив**	**Власник**	**Загроза**	**Уразливість**	**Імовірність виникнення**	**Збиток**	**Величина ризику**	**Обране забезпечення**
Північна К1	S.10	Операційна система	Системний адміністратор	Віруси	Уразливість ОС	5	5	25	
Юридична служба	P.35	Юрист-консульт	Керівник відділу персоналу	Неповноцінне врахування інтересів підприємства при оформленні договору	Незнання законодавства	3	5	15	
Відділ проектування	D.156	Проектного продукту	Керівник відділу проектування	Потрапляння проекту до конкурентів	Звільнення ключового співробітника	3	9	27	

Таблиця 3.41. Приклад шкали для визначення ймовірності

Імовірність виникнення	Опис
Дуже низька	Малоімовірно
Низька	1 раз на 3 роки
Середня	1 раз на рік
Висока	Декілька разів на рік
Дуже висока	Раз на місяць і частіше

Таблиця 3.42. Приклад шкали для визначення впливу збитків на оцінку ризиків

Потенційні збитки	Бізнес-функції / фінансовий стан	Відповідність законодавству	Репутація / імідж	Персональна інформація
Низький	Невеликі проблеми (величина збитку до X)	Незначні порушення законодавства (адміністративна відповідальність, величина штрафу до X)	Невеликі, малозначні проблеми	Невдоволення одного клієнта або невеликої групи людей
Середній	Фінансові проблеми (величина збитку до XXX)	Порушення законодавства (адміністративна величина штрафу до XXX)	Негативна реакція клієнтів, партнерів і / або інвесторів по відношенню до підприємства	Невеликі проблеми
Високий	Серйозні фінансові проблеми / збитковість підприємства (величина збитку більше XXX)	Грубе порушення законодавства (кримінальна відповідальність, адміністративна - величина штрафу більша XXX)	Сильне негативне ставлення клієнтів, партнерів і / або інвесторів до підприємства	Серйозні проблеми
Дуже високий	Може призвести до банкрутства	Може привести до закриття підприємства	Загроза подальшому існуванню підприємства	Серйозні глобальні проблеми

Score) та контекстної (Environmental Score) (в БД CVSS доступний в двох версіях – v2.0 [63] та v3.0 [64]);

– уразливі версії ПЗ;

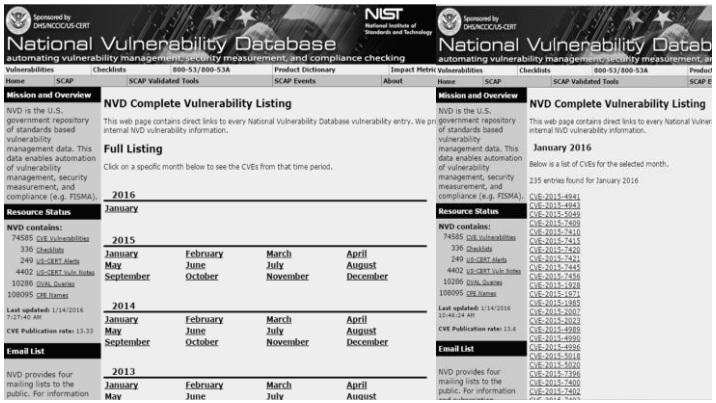


Рис. 3.26. Список уразливостей на сайті NVD

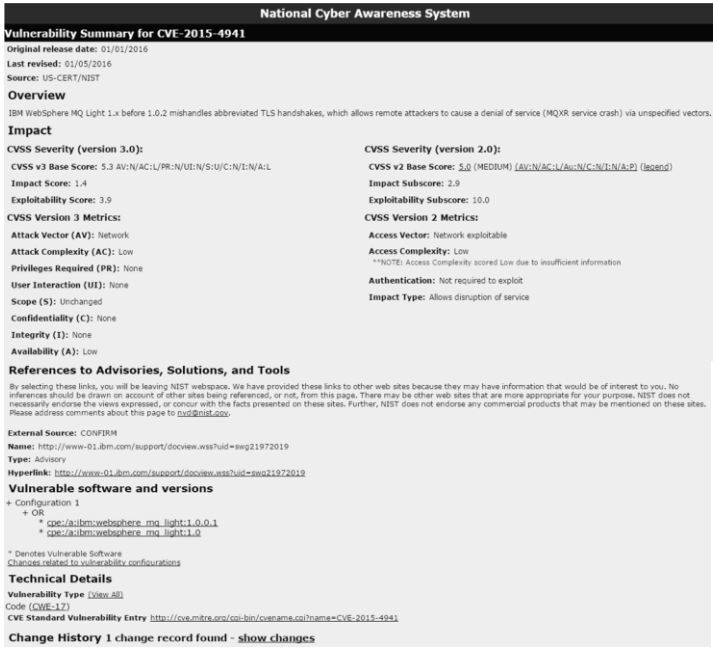


Рис. 3.27. Приклад представлення уразливостей в NVD

Таблиця 3.35. Значення показників оцінок CVSS v2.0

МГ	Множина показників	Набори символьних значень показників	Числові значення відповідних показників
Базова	**AV**	L; A; N	0,395; 0,646; 1
	AC	H; M; L	0,35; 0,61; 0,71
	Au	M; S; N	0,45; 0,56; 0,704
	C; I; A	N; P; C	0; 0,275; 0,66
Часова	**E**	ND; U; POC; F; H	1; 0,85; 0,9; 0,95; 1
	RL	ND; OF; TF; W; U	1; 0,87; 0,9; 0,95; 1
	RC	ND; UC; UR; C	1; 0,90; 0,95; 1
Середовище оточення	**CDP**	ND; N; L; LM; MH; H	0; 0; 0,1; 0,3; 0,4; 0,5
	TD	ND; N; L; M; H	1; 0; 0,25; 0,75; 1
	CR; IR; AR	ND; L; M; H	1; 0,5; 1; 1,51

– CWE категорія;
– додаткові посилання;
– інші відомості [57].

Відзначимо, що умова існування уразливості зберігається у вигляді диз'юнктивної нормальної форми. Розглянемо більш детально кожну з версій CVSS та визначимо їх відмінності.

CVSS v2.0. Метрики та їх параметри, що входять в стандарт CVSS v2.0 [63] показані на рис. 3.28. У цій версії здійснюється стандартизоване оцінювання уразливостей, система є відкритою і орієнтована на визначення пріоритетних ризиків. Кожна МГ визначає характеристики уразливості. Наведемо ці групи (див. рис. 3.28).

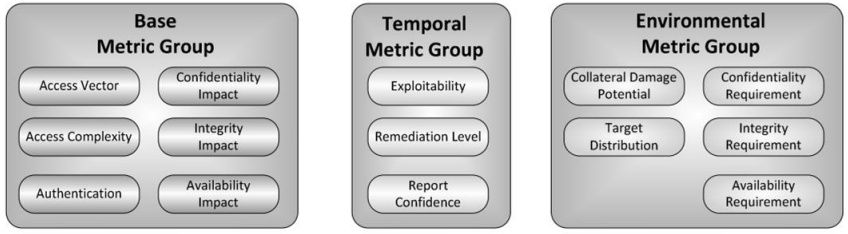


Рис. 3.28. МГ CVSS v2.0

Base Score Metrics (метрики базових оцінок) – характеристики уразливостей, які є постійними протягом великого періоду часу у користувацьких середовищах і не залежать від них. Також вони

Уразливості можуть бути пов’язані з властивостями активу, які можуть використовуватися способом і з метою, що відрізняються від тих, які планувалися під час придбання або створення активу. Уразливості, що виникають з різних джерел, підлягають розгляду, наприклад, ті які є зовнішніми або внутрішніми по відношенню до активу.

Ідентифікація наслідків

Ця діяльність ідентифікує шкоду для організації або наслідки для організації, які можуть бути обумовлені сценарієм інциденту, що надається загрозою, що використовує певну уразливість в інциденті ІБ.

Вплив сценаріїв інцидентів слід визначати, використовуючи критерії впливу, дійсні протягом діяльності, пов’язаної з встановленням контексту. Він може стосуватися одного або більшої кількості активів чи частини активу. Тому активам може призначатися цінність в залежності від їх фінансової вартості і через збитки для бізнесу в разі їх псування або компрометації.

Наслідки можуть бути тимчасовими або постійними, як у випадку руйнування активів.

Організації повинні визначати операційні наслідки сценаріїв інцидентів на основі (але не обмежуючись):

– часу на розслідування і відновлення;
– втрат (робочого) часу;
– упущеної можливості;
– охорони праці та безпеки;
– фінансових витрат на специфічні навички, необхідні для усунення несправності;

репутації і іншого «невловимого капіталу» [20].

Визначити підхід організації до оцінки ризику:

– вплив ймовірності виникнення на оцінку ризиків (табл. 3.41);
– вплив збитку на оцінку ризиків (табл. 3.42);
– ранжування і розрахунок ризиків (табл. 3.43).

– перегляд документів, що містять інформацію про засоби контролю (наприклад, плани обробки ризиків). Якщо процеси менеджменту ІБ задокументовано належним чином, то всі існуючі або заплановані засоби контролю і стан їх реалізації повинні бути доступні;

– перевірка разом з людьми, які відповідають за ІБ (наприклад, службовець, який займається забезпеченням ІБ, службовець, відповідальний за безпеку ІС, комендант будівлі або керівник робіт) і користувачами, які засоби контролю дійсно реалізовані для розглянутого інформаційного процесу або ІС;

– обхід будівлі з проведенням огляду фізичних засобів контролю, порівняння реалізованих засобів контролю з переліком тих, які повинні бути, і перевірка реалізованих засобів контролю на предмет правильної і ефективної роботи;

– розгляд результатів внутрішніх аудитів.

Ідентифікація уразливості

Уразливості можуть бути ідентифіковані в наступних областях:

– організація робіт;
– процеси і процедури;
– усталені норми управління;
– персонал;
– фізичне середовище;
– апаратні засоби, програмне забезпечення та апаратура зв'язку;
– залежність від зовнішніх сторін.

Наявність уразливості не завдає шкоди саме по собі, так як необхідна наявність загрози, яка скористається нею. Уразливість, яка не має відповідної загрози, може не вимагати впровадження засобів контролю, але повинна усвідомлюватися і піддаватися моніторингу на предмет вимірювань.

Треба зазначити, що невірно реалізований або неправильно функціонуючий засіб контролю, який неправильно використовується, сам може бути уразливістю. Засіб контролю може бути ефективним чи неефективним в залежності від середовища, в якому він функціонує. І навпаки, загроза, яка не має відповідної уразливості, може не призводити до ризику.

описують складність експлуатації уразливості і потенційний збиток для конфіденційності, цілісності та доступності. МГ, що використовуються, складаються з наступних показників:

– вектор доступу (Access Vector (**AV**));
– складність доступу (Access Complexity (**AC**));
– аутентифікація (Authentication (**Au**));
– вплив на конфіденційність (Confidentiality Impact (**C**));
– вплив на цілісність (Integrity Impact (**I**));
– вплив на доступність (Availability Impact (**A**)).

Temporal Score Metrics (метрики часових оцінок) – характеристики уразливості, які змінюються з плином часу в позакористувальницьких середовищах. Вони вносять в загальну оцінку поправки на повноту наявної інформації про уразливість, зрілість експлуатованого коду (при його наявності) та доступність виправлень. Її показники:

– можливість використання (Exploitability (**E**));
– рівень виправлення (Remediation Level (**RL**));
– достовірність звіту (Report Confidence (**RC**)).

Environmental Score Metrics (метрики контекстних оцінок) – характеристики уразливості, які актуальні та унікальні для середовища конкретного користувача. За допомогою цих метрик експерти з безпеки можуть внести в результуючу оцінку поправки з урахуванням характеристик інформаційного середовища. Група МГ складається з показників загальних модифікаторів (General Modifiers):

– можливості непрямого збитку (Collateral Damage Potential (**CDP**));
– цільовий розподіл (Target Distribution (**TD**)),

а також модифікатори впливових показників (Impact Subscore Modifiers):

– вимога конфіденційності (Confidentiality Requirement (**CR**));
– вимога цілісності (Integrity Requirement (**IR**));
– вимога доступності (Availability Requirement (**AR**)).

У таблиці 3.35 для кожної МГ (метрик оцінок) до кожної множини показників наведені низки символьних значень та відповідні їм числові показники. Також кожному символьному значенню визначена відповідна йому лінгвістична інтерпретація:

– для **AV** (Access Vector – вектор доступу):
  – L – «Локальний доступ»;
  – A – «Сполучена мережа»;
  – N – «Мережа»,
– для **AC** (Access Complexity – складність доступу):
  – H – «Висока»;
  – M – «Середня»;
  – L – «Низька»,
– для **Au** (Authentication – аутентифікація):
  – M – «Багаторазова»;
  – S – «Одноразова»;
  – N – «Відсутня»,
– для **C** (Confidentiality Impact – вплив на конфіденційність), **I** (Integrity Impact – вплив на цілісність) та **A** (Availability Impact – вплив на доступність):
  – N – «Відсутній»;
  – P – «Частковий»;
  – C – «Повний»,
– для **E** (Exploitability – можливість використання):
  – ND – «Не визначена»;
  – U – «Теоретична (немає доказів)»;
  – POC – «Експериментальна»;
  – F – «Функціональна»;
  – H – «Висока»,
– для **RL** (Remediation Level – рівень виправлення):
  – ND – «Не визначено»;
  – OF – «Офіційний патч»;
  – TF – «Тимчасове рішення»;
  – W – «Рішення на основі порад та рекомендацій»;
  – U – «Відсутні»,
– для **RC** (Report Confidence – достовірність звіту):
  – ND – «Не визначена»;
  – UC – «Носить гіпотетичний характер»;
  – UR – «Не опрацьована»;
  – C – «Підтверджена»,

– слабка система контролю доступу до інформаційних ресурсів сторонніх осіб.

4) Часткова або повна втрата інформації по розробці нового проекту:
  – пожежа в архіві;
  – вихід з ладу жорсткого диска на сервері;
  – звільнення з роботи ключового учасника, керівника проекту.

Ідентифікація існуючих засобів контролю

Ідентифікація існуючих засобів контролю повинна бути зроблена, аби уникнути непотрібної роботи або витрат, наприклад, при дублюванні засобів контролю. Крім того, під час ідентифікації існуючих засобів контролю слід провести перевірку, щоб упевнитися, що засоби контролю функціонують правильно – посилання на вже існуючі звіти по аудиту СМІБ повинні обмежувати час, що витрачається на цю задачу. Якщо засоби контролю не працюють, як очікувалося, це може стати причиною уразливості. Слід приділити увагу ситуації, коли вибрані засоби контролю (або стратегія) відмовляються працювати і тому потрібні додаткові засоби контролю для ефективного розгляду ідентифікованого ризику. У СМІБ, відповідно до ISO/IEC 27001, це підтримується виміром ефективності засобів контролю. Одним із способів кількісно оцінити дію засобів контролю – подивитися, як воно зменшує ймовірність загрози і простоту використання уразливості або вплив інциденту. Перегляд, здійснюваний менеджерами і звіти з аудиту, також забезпечують інформацію про ефективність існуючих засобів контролю.

Засіб контролю, які планується реалізувати у відповідність з планами реалізації обробки ризику, повинні враховуватися тим же самим способом, який вже був реалізований.

Існуюче або запланований засіб контролю може ідентифікуватися як неефективний, або недостатній, або необґрунтований. Якщо його визнано необґрунтованим або недостатнім, засіб контролю необхідно перевірити, щоб визначити чи варто його видалити, замінити його іншим, більш відповідним, або варто залишити його на місці, наприклад, з економічно-вартісних причин.

Для ідентифікації існуючих або планованих засобів контролю можуть бути корисні наступні заходи:

Використовуючи реєстри загроз або результати колишніх оцінок загроз, не слід забувати про те, що відбувається постійна зміна значущих загроз, особливо, якщо змінюються бізнес-середовище або ІС [20].

Приклади інформаційних загроз (рис. 3.49)

1) Несвоєчасність отримання інформації, необхідної для прийняття управлінських рішень:

– зміна рівня продажів;
– зміна потужності обладнання;
– зміна переваг споживача;
– показники роботи конкурентів;
– інформація про виконання виробничого плану;
– інформація про запаси на складі.

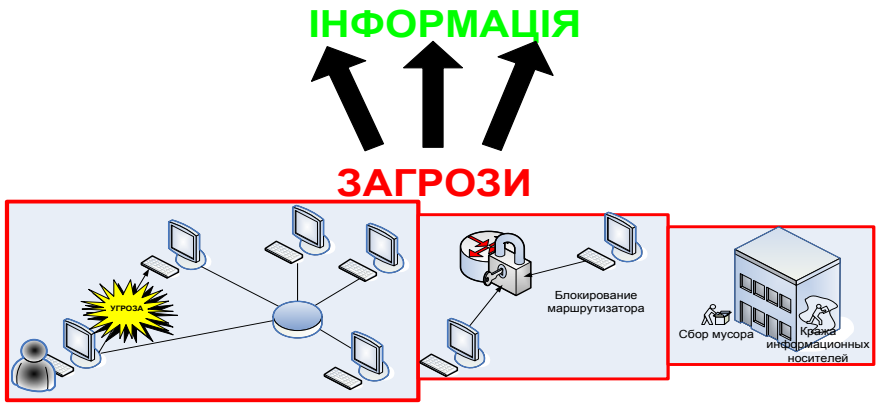


Рис. 3.49. Приклади інформаційних загроз

2) Використання старих версій адміністративних документів:

– новий співробітник на підприємстві взяв стару версію процедури і працює по ній;

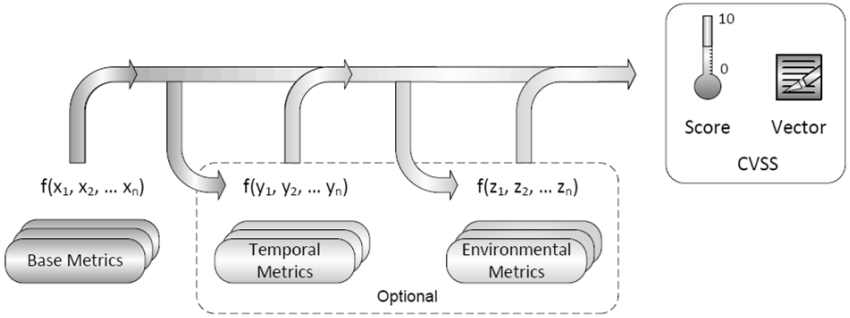
– затримка у виконанні контракту через виконання дій, скасованих в нових правилах.

3) Потрапляння комерційної інформації до конкурентів:

– корислива або безкорислива передача інформації співробітником підприємства;

– використання конкурентом технічних засобів зняття інформації;

– для **CDP** (Collateral Damage Potential – можливість непрямого збитку):
  – ND – «Не визначена»;
  – N – «Відсутня»;
  – L – «Низька»;
  – LM – «Низько – середня»;
  – MH – «Може бути – висока»;
  – H – «Висока»,
– для **TD** (Target Distribution – цільовий розподіл):
  – ND – «Не визначений»;
  – N – «Відсутній»;
  – L – «Низький»;
  – M – «Середній»;
  – H – «Високий»,
– для **CR** (Confidentiality Requirement – вимога конфіденційності), **IR** (Integrity Requirement – вимога цілісності) та **AR** (Availability Requirement – вимога доступності):
  – ND – «Не визначена»;
  – H – «Висока»;
  – M – «Середня»;
  – L – «Низька» (також див. рис. 3.28 і 3.29).



Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Рис. 3.29. CVSS v2.0 – МГ і вектора

Після присвоєння символьних значень конкретних чисел здійснюється обчислення рейтингу (в межах [0; 10]) та створення вектора (як показано на рис. 3.27) AV: N / AC: L / Au: N / C: N / I: N / A: P, який відображає «відкритість» структури. Фактично, це текстовий рядок, який містить значення, присвоєні кожній метриці і використовується для взаємодії оцінок. Відзначимо, що таким чином вектор повинен відображатися з урахуванням уразливості [63].

Тимчасові та контекстні МГ опційні і застосовуються для більш точної оцінки небезпеки, яку представляє дана уразливість для конкретної інфраструктури. Значення МГ відображається у вигляді пари (див. рис. 3.29) з вектора (конкретні значення окремих показників) і числового значення, розрахованого на основі всіх показників за допомогою формул стандарту [63].

Використання Temporal дозволяє об'єднати тимчасові і базові показники, які відображаються на шкалу з межами [0; 10]. При цьому, часова оцінка буде не вище базової, але не менше її на 33% [63]. На рис. 3.30 показаний вбудований калькулятор показників CVSS v2.0 в Веб-інтерфейс NVD [57].

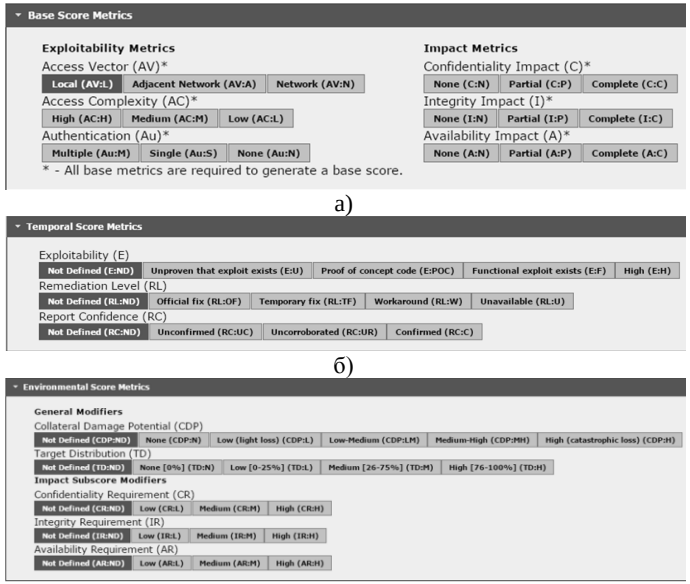


Рис. 3.30. Інтерфейс вмонтованого калькулятора CVSS v2.0 в Веб-інтерфейс NVD МГ: а) Базова, б) Часова, в) Контекстна

різні методи оцінки. На даному етапі можна використати, наприклад, метод Делфі. Особливістю якого є: наочність, многорівнева структура та анонімність. Цей метод ґрунтується на послідовності дій таких, як опитування, інтерв'ю, мозковий штурм. Головне добитися максимального консенсусу при визначенні правильного рішення. Базовим принципом методу являється те, що певна кількість незалежних експертів краще оцінює і передбачає результат, чим структурована група особистостей [69].

Ідентифікація загроз

Загроза має потенціал заподіяння шкоди активів, а, отже, і організаціям, таким як інформація, процеси і системи. Загрози можуть бути природного походження або від дій людей, вони можуть бути випадковими або навмисними. Повинні бути ідентифіковані випадкові і навмисні джерела загроз. Загроза може виникати як з самої організації, так і поза її межами. Загрози повинні ідентифікуватися загалом, а також за видом (наприклад, неавторизовані дії, фізичний збиток, технічні збої), а потім, де це доречно, окремі загрози ідентифікуються всередині родового класу. Це означає, що жодна загроза, включаючи несподівані, не буде упущена, але обсяг необхідної роботи, незважаючи на це, обмежений.

Деякі загрози можуть впливати більш ніж на один актив. У таких випадках вони можуть бути причиною різних впливів, в залежності від того, на які активи здійснюється вплив.

Вхідні дані для ідентифікації та вимірювання ймовірності виникнення загроз можуть бути отримані від власників активів або користувачів, персоналу відділу кадрів, керівництва організації та фахівців у сфері ІБ, експертів в сфері фізичної безпеки, юридичного відділу та інших структур, включаючи правові органи, метеорологічні служби, страхові компанії, національні урядові установи. При розгляді загроз повинні враховуватися аспекти середовища і культури.

Внутрішній досвід, отриманий в результаті інцидентів, і минулі оцінки загроз повинні бути враховані в поточній оцінці. Може бути доцільно розглянути інші реєстри загроз (можливо, специфічних для організації або бізнесу), щоб заповнити перелік спільних загроз, де це має значення. Реєстри та статистику загроз можна отримати від промислових організацій, національних урядів, правових органів, страхових компаній і т.д.

– рівні забезпечення;
– максимальний час недоступності;
– власник активу;
– місце знаходження активу;
– категорія активу.

Найкраще використовувати типові (стандартні) назви активів. Наприклад, «Персональний комп'ютер бухгалтерії №12» можна задекларувати так: «ПК №12 тип Б». Це дає змогу отримати в результаті просту і наочну таблицю. Виділяють такі три рівні забезпечення: конфіденційності, цілісності, доступності, тобто необхідно оцінити можливі втрати, що понесе організація. Шкалу рівнів забезпечення можна виконувати в грошовому еквіваленті та за допомогою системи рівнів. Для базової оцінки ризиків достатньо трьох рівневої шкали оцінки градації (низький, середній, високий). При виборі рівнів забезпечення слід враховувати:

– чим менша кількість рівнів, тим нижча точність оцінювання;

– чим більша кількість рівнів, тим складнішим стає оцінювання.

Виходячи з даного твердження потрібно сказати, що надмірно велика градація ризиків активів не завжди є доцільною. Максимальний час недоступності – час на протязі якого дозволяється недоступність інформаційного активу. Власником активу варто призначати особу, яка реально працює з активом і здатна впливати на властивості і стан активу. Місцезнаходження активу найчастіше визначають територіально відповідно до проекту будівлі. Наприклад, «корпус №5», «Бухгалтерія», «НДЧ». Категоріювання активів дає змогу згрупувати схожі активи і спростити роботу з ними. Такими категоріями можуть бути: «Паперові документи (ПД)», «Електронні документи (ЕД)», «Програмне забезпечення (ПЗ)», «Комп'ютерна техніка (КТ)», «Мережеве обладнання (МО)», «Допоміжне обладнання (ДО)», «Персонал (П)», «Віртуальна інформація (ВІ)». Даний процес створює певну складність, оскільки цінність активів визначається на основі експертних оцінок їх власників. На даному етапі часто проводять обговорення між консультантами з розробки системи безпеки та власником активів. Це дозволяє власникам активів, зрозуміти яким чином слід визначити вартість активів з точки зору ІБ. Для власників активів розробляють

CVSS v3.0. Калькулятор CVSS v3.0 є розвитком CVSS v2.0. На рис. 3.31 схематично показані зміни внесені в третю версію. Для прикладу розглянемо уразливість у віртуальній машині, яка наражає на небезпеку основну операційну систему (ОС). Тут уразливим компонентом є віртуальна машина, а впливовим компонентом – ОС хоста. Це пов'язано з тим, що ці два компоненти незалежно управляють правами на обчислювальні ресурси. Віртуальна машина (як показано на рис. 3.31) управляється «Адміністратором А», в той час як ОС хоста управляється «Адміністратором В». Коли два адміністратора одночасно експлуатують компоненти, то це може ініціювати створення уразливості. В цьому випадку CVSS вважає, що зміни вже відбулися. Ця умова тепер відбивається в нових МГ [64].

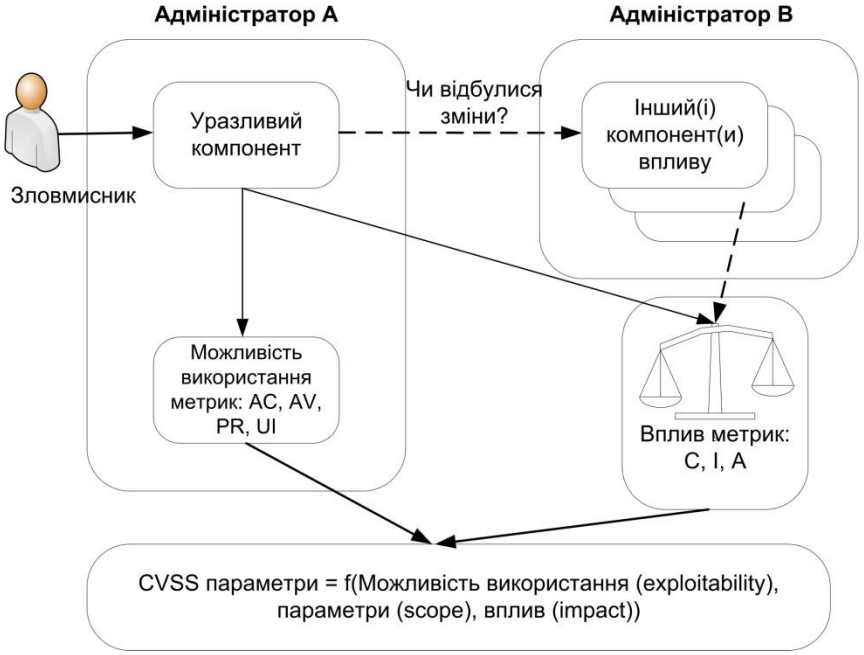


Рис. 3.31. Зміни в CVSS v3.0

В межах стандарту вводяться два наступних базових поняття:

− уразливий компонент (vulnerable component) – компонент ІС, що містить уразливість і бере участь в процесі експлуатації;

– атакуючий компонент (impacted component) – компонент ІС, базові характеристики безпеки якого (конфіденційність, цілісність, доступність) можуть бути порушені у разі успішній реалізації атаки.

Як правило, уразливий та атакуючий компоненти збігаються, але існують класи уразливостей, для яких це правило не працює, наприклад:

– вихід за межі «пісочниці» додатка;

– отримання доступу до призначених для користувача даних, збережених в браузері, через уразливість у Веб-додатку (XSS);

– вихід за межі гостьової віртуальної машини та ін.

У цій версії метрики експлуатації розраховуються для уразливого компонента, а метрики впливу для атакуючого. Версія CVSS v2 не дозволяла відображати ситуацію, при якій уразливий компонент і той, який атакується, розрізняються [64, 65].

У CVSS v3.0 вектор доступу (Access Vector в v2.0) був перейменований в вектор атаки, але, як і раніше, відображає «віддаленість» зловмисника по відношенню до уразливих компонентів. Іншими словами, чим більш віддаленим зловмисник є відносно уразливого компонента (з точки зору логічної та фізичної віддаленості мережі), тим більше буде базова оцінка. Крім того, цей показник розрізняє локальні атаки, які вимагають локального доступу до системи (наприклад, атака на програмний застосунок) і фізичні, які вимагають фізичного доступу до платформи для використання уразливості (наприклад, з FireWire, USB або jailbreaking атака) [63].

Зміни стосувалися і поняття значення показника «Local», яке раніше описувало будь-які дії, що не стосуються мережі. У новому стандарті вводиться наступний розподіл значень цього показника:

– Local (для експлуатації атакуючому потрібна локальна сесія або певні дії з боку легітимного користувача).

– Physical (атакуючому необхідний фізичний доступ до уразливої підсистеми [65]).

Також зміни відбулися і щодо показника **AC**, тобто складність експлуатації уразливості, що є якісною оцінкою складності проведення атаки. Чим більше умов має бути дотримано для експлуатації уразливості, тим вище складність [65]. Тут були об'єднані два значення показника «Low» та «Medium». Таким чином, складність

б) ЕІ може оперативно створюватись;

в) ЕІ може накопичуватися у великих обсягах, при цьому представляючи зручний та оперативний доступ до необхідної її частини.

Негативні:

а) ЕІ легко пошкодити або знищити;

б) ЕІ може легко потрапити в руки конкурента.

Об’єктом СМІБ є інформаційні активи, тобто матеріальні або нематеріальні об’єкти, які є інформацією або містять інформацію, або необхідні для оброблення інформації. Наприклад, одним активом є: системний блок + монітор + клавіатура + муніпулятор + всі електронні документи, які розміщенні на дисках персонального комп’ютера (ПК) + все ПЗ, яке встановлене на ПК. Інформаційні активи – це:

– бази даних і файли даних;
– договори і домовленості;
– системна документація;
– науково-дослідна інформація;
– довідкова інформація, методичні вказівки, інструкції;
– навчальний матеріал;
– процедури експлуатації;
– плани забезпечення неперервності функціонування;
– заходи щодо ліквідації неполадок;
– контрольні журнали;
– архівна інформація.

Інформаційні активи володіють основними властивостями фінансових і матеріальних активів підприємства. Загалом цінність інформаційних активів набагато більша за фінансові активи підприємства. Захист інформаційних активів залишається одним з пріоритетних на сьогоднішній день.

Розглянемо приклад методики опису інформаційних активів на основі стандартів ISO/IEC 27001, ISO/IEC 13335-3, який передбачає створення реєстру інформаційних активів організації. Згідно методики створюється реєстр активів, тобто подається розгорнута таблиця в якій відображаються існуючі активи організації (таблиця). Під час опису активів використовуються такі атрибути:

– назва активу;

може не мати права власності на актив, але він несе відповідальність за його отримання, розробку, підтримку, використання і безпеку. Найчастіше власник активу є найбільш підходящою особою, яка спроможна визначити реальну цінність активу для організації [20].

Інформаційний актив (ресурс) – матеріальний або нематеріальний об'єкт, який:

– є інформацією або містить інформацію;
– має цінність для організації.

Приклади простих активів:

а) законодавча база (наприклад, інструкції НБУ тощо);
б) проекти продуктів;
в) рекламні пропозиції;
г) договори з клієнтами (наприклад, кредитні, депозитні тощо);
д) кредитні пакети (наприклад, дані про позичальника, договори тощо);
е) касові ордери, меморіальні ордери;
ж) фінансова звітність.

Приклади складних активів:

а) ноутбук керівника підприємства з інформацією про фінансовий стан банку;
б) сервер, який містить інформацію про рахунки клієнтів;
в) архів (приміщення) з касовими ордерами, меморіальними ордерами тощо;
г) президент банку, в голові у якого план перспективної і оперативної діяльності банку.

Властивості інформації (активів):

1) інформація важлива в певний момент часу;
2) інформація підприємства становить інтерес для третіх осіб (клієнтів, постачальників, конкурентів);
3) обсяг інформації на підприємстві великий і постійно зростає;
4) інформаційні потоки на підприємстві перебувають у постійному русі;
5) інформаційні потоки формують ІС підприємства.

Електронна інформація (ЕІ) має додаткові властивості:

Позитивні:

а) ЕІ можна оперативно доставити в будь-яку точку світу;

доступу була представлена в двох параметрах – складність атаки і взаємодія користувача [64]. Поняття «складність» саме по собі суб'єктивне, а тому цей параметр, завжди трактувався експертами порізному. Наприклад, для уразливостей, що дозволяють реалізувати атаку «Людина посередині» (активна атака [63]), в базі NVD можна зустріти різні варіанти оцінки **AC**.

Тепер для полегшення тлумачення даного параметру пропонуються тільки два ступеня складності «High» та «Low», а також більш чітко прописані критерії віднесення до них уразливостей. Зокрема, уразливість, що дозволяє реалізувати активну атаку, запропоновано відносити до значення показника «High». Чинники, що враховуються в CVSS v2 параметром **AC**, в новому стандарті розкривається двома показниками – Attack Complexity та User Interaction [65].

У CVSS v3.0 з'явився новий показник – «необхідні привілеї» (Privileges Required), який замінює показник «аутентифікації» в v2.0 (аутентифікація/необхідний рівень привілеїв – чи потрібна аутентифікація для проведення атаки, і якщо потрібна, то яка саме [65]). Необхідні привілеї, відображають рівень доступу, необхідний для успішної атаки. Зокрема, значення показників «High», «Low» та «None» відображають привілеї, необхідні зловмисникові для того, щоб скористатися уразливістю. Підхід до розрахунку показника заснований на кількості незалежних процесів аутентифікації, які потрібно пройти атакуючому [65]. Всі інші зміни в CVSS v3.0 відображені в таблиці 3.36 [64]. Тут, за аналогією з табл. 3.36, для кожної МГ по кожній множині показників наведені низки символьних значень і відповідні їм числові показники.

Крім цього, кожному символьному значенню визначена відповідна йому лінгвістична інтерпретація

– для **AV** (Attack Vector – вектор атаки):
  – N – «Мережа»;
  – A – «Сполучена мережу»;
  – L – «Локальний доступ»;
  – P – «Фізичний доступ»,
– для **AC** (Attack Complexity – складність атаки):
  – H – «Висока»;
  – L – «Середня»,

Таблиця 3.36. Значення показників оцінок CVSS v3.0

МГ	Множина показників	Низки символьних значень показників	Числові значення відповідних показників
Базова	**AV**	N; A; L; P	0,85; 0,62; 0,55; 0,2
	AC	H; L	0,77; 0,44
	PR	H; L; N	0,85; 0,62 (або 0,68*); 0,27 (або 0,50*)
	UI	N; R	0,85; 0,62
	S	U; C	-
	C; I; A;	N; L; H;	0; 0,22; 0,56
Часова	**E**	U; P; F; H; X	0,91; 0,94; 0,97; 1; 1
	RL	O; T; W; U; X	0,95; 0,96; 0,97; 1; 1
	RC	U; R; C; X	0,92; 0,96; 1; 1
Середовища оточення	**CR; IR; AR**	L; M; H; X	0,5; 1; 1,5; 1
Модифікована базова	**MAV; MAC; MPR; MUI; MS; MC; MI; MA**	Мають ті ж символьні та числові значення показників, що і відповідні немодифіковані показники в базовій МГ, а також «Not Defined» (за замовчуванням)	
*якщо область дії (S) / модифікована область дії (MS) змінюється			

– для **PR** (Privileges Required – необхідні повноваження):
  – H – «Високі»;
  – L – «Середні»;
  – N – «Відсутні»,
– для **C** (Confidentiality Impact – вплив на конфіденційність), **I** (Integrity Impact – вплив на цілісність) та **A** (Availability Impact – вплив на доступність):
  – H – «Високий»;
  – L – «Середній»;
  – N – «Відсутній»,
– для **UI** (User Interaction – взаємодія з користувачем):
  – N – «Відсутня»;
  – R – «Потрібна»,
– для **S** (Scope – область дії):
  – U – «Без змін»;

недостатню інформацію для оцінки ризику, потім проводиться подальший детальний аналіз, ймовірно, для частин повної сфери і, можливо, використовуючи інший метод.

Вибір власного підходу до оцінки ризику на основі завдань і цілі оцінки ризику залежить від самої організації [20].

Про підходи до оцінки ризику ІБ йшлося в підрозділах 3.1 та 3.2.

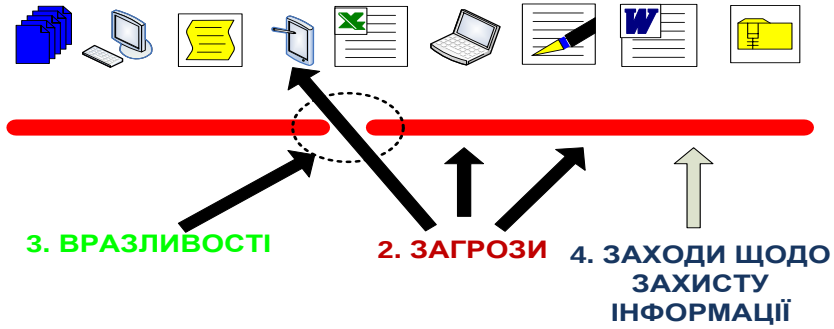


Рис. 3.48. Процес оцінювання ризиків

Метою ідентифікації ризику є визначення того, що може бути причиною нанесення потенційного збитку, для отримання уявлення про те, як, де і чому це може мати місце. Етапи, описані нижче, повинні збирати вхідні дані для діяльності щодо кількісного оцінювання ризику [20].

Ідентифікація активів

Активом є щось, що має цінність для організації і, отже, потребує захисту. При ідентифікації активів слід мати на увазі, що ІС складається не тільки з апаратних і програмних засобів.

Ідентифікацію активів слід здійснювати на відповідному рівні деталізації, що забезпечує достатню інформацію для оцінювання ризику. Рівень деталізації, який використовується для ідентифікації активів, впливає на загальний обсяг інформації, зібраної під час оцінки ризику. Цей рівень може бути більш деталізований при подальших ітераціях оцінки ризику.

Для кожного активу повинен бути визначений власник, щоб забезпечити облік і відповідальність за кожен актив. Власник активу

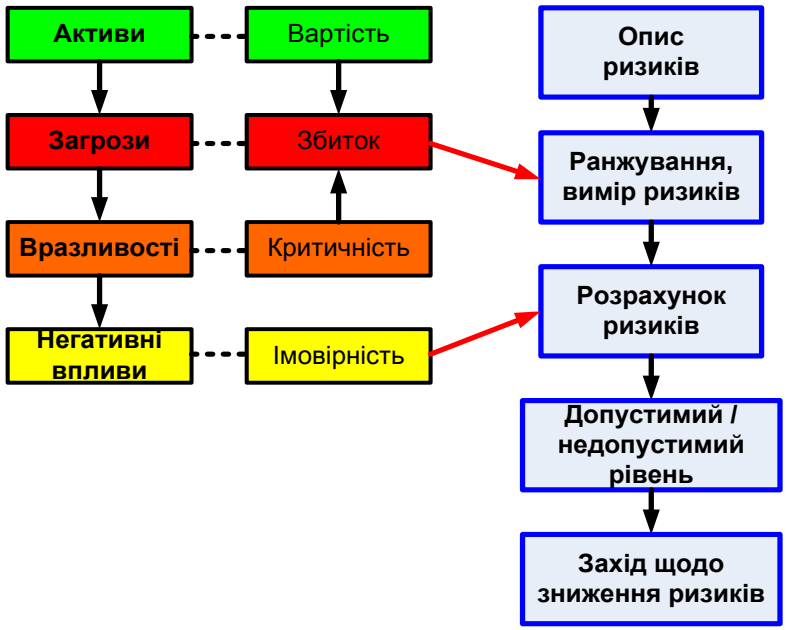


Рис. 3.47. Опис ризик-менеджменту

Оцінка ризику (см. рис. 3.48) складається з наступних заходів:

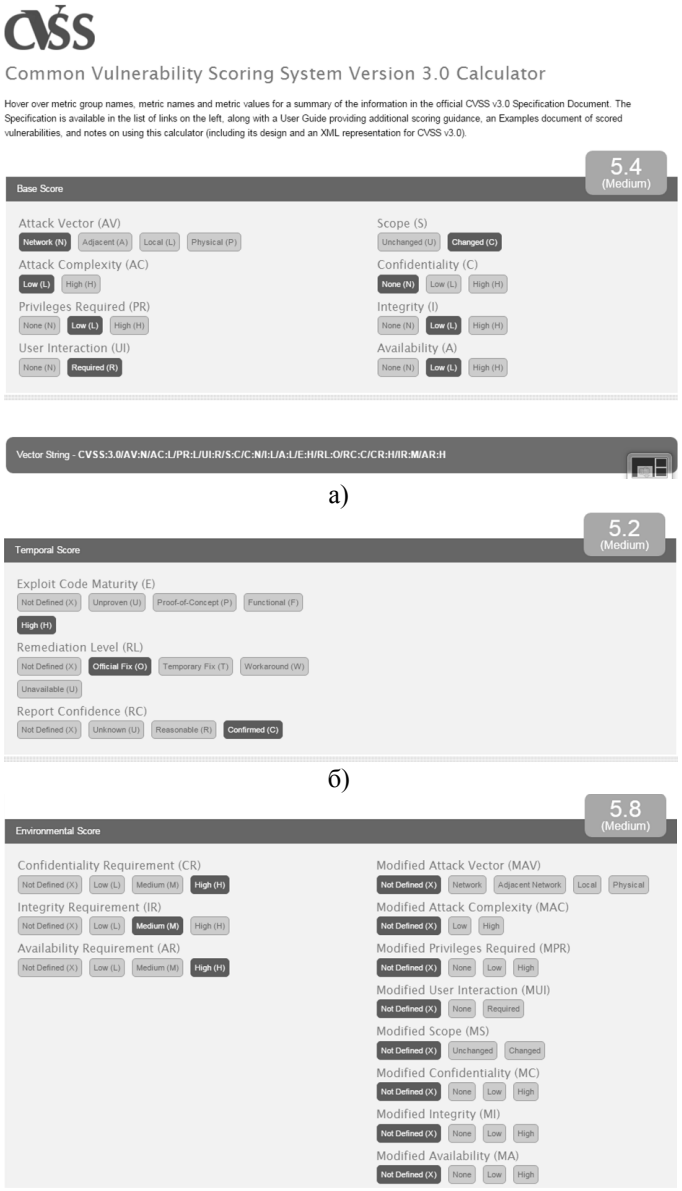
– ідентифікацію ризику;
– аналіз ступеня ризику;
– оцінювання ризику.

Оцінка ризику визначає цінність інформаційних активів, ідентифікує застосовні загрози і уразливості, які існують (або можуть існувати), ідентифікує існуючі засоби контролю і їх вплив на ідентифіковані ризики, визначає потенційні наслідки і, нарешті, розставляє виведені ризики відповідно до пріоритетів і ранжує їх по критеріям оцінювання ризику, зафіксованим під час установки контексту.

Оцінювання ризику часто проводиться з використанням двох (або більше) ітерацій. Спочатку проводиться високорівневе оцінювання для ідентифікації потенційно високі ризики, які виправдовують подальше оцінювання. Наступна ітерація може містити подальший поглиблений розгляд потенційно високих ризиків, виявлених у процесі початкової ітерації. У тих випадках, коли це надає

  – C – «Змінена»,
– для **E** (Exploitability – можливість використання):
  – U – «Теоретична (немає доказів)»;
  – P – «Експериментальна»;
  – F – «Функціональна»;
  – H – «Висока»;
  – X – «Не визначена»,
– для **RL** (Remediation Level – рівень виправлення):
  – O – «Офіційний патч»;
  – T – «Тимчасове рішення»;
  – W – «Рішення на основі порад та рекомендацій»;
  – U – «Відсутні»;
  – X – «Не визначені»,
– для **RC** (Report Confidence – достовірність звіту):
  – U – «Відсутня»;
  – R – «Обгрунтована»;
  – C – «Підтверджена»;
  – X – «Не визначена»,
– для **CR** (Confidentiality Requirement – вимога конфіденційності), **IR** (Integrity Requirement – вимога цілісності) та **AR** (Availability Requirement – вимога доступності):
  – L – «Низькі»;
  – M – «Середні»;
  – H – «Високі»;
  – X – «Не визначені».

Модифікована базова група метрик описується показниками **MAV** (Modified Attack Vector – модифікований вектор атаки), **MAC** (Modified Attack Complexity – модифікована складність атаки), **MPR** (Modified Privileges Required – модифіковані необхідні повноваження), **MUI** (Modified User Interaction – модифікована взаємодія з користувачем), **MS** (Modified Scope – модифікована область дії), **MC** (Modified Confidentiality – модифікована конфіденційність), **MI** (Modified Integrity – модифікована цілісність) та **MA** (Modified Availability – модифікована доступність) (також див. рис. 3.31 і 3.32). На рис. 3.32 показаний вбудований калькулятор показників CVSS v3.0 у Веб-інтерфейс.



в)

Рис. 3.32. Інтерфейс вбудованого калькулятора CVSS v3.0 МГ: а) Базова; б) Часова; в) Середовище оточення

3) визначає рівні ризиків;

д) оцінює ризики ІБ.

1) порівнює результати аналізу ризиків з критеріями ризиків, визначеними в п. а);

2) визначає пріоритети проаналізованих ризиків для оброблення ризиків.

Організація повинна зберігати документовану інформацію стосовно процесу оцінювання ризиків ІБ [68].

Ризик являє собою комбінацію наслідків, що випливають з небажаної події, і ймовірності виникнення події.

Ризик – це комбінація ймовірності події та її наслідків [20]**.**

Як приклад, можна розглянути його як: R = S * E (R = Ризик, S = Розмір збитку, E = Імовірність події)

Ризик-менеджмент приділяє основну увагу превентивним заходам або заходам, що пом'якшують наслідки.

Завдання ризик-менеджменту – це ідентифікація ризиків і управління ризиками.

Система управління ризиками дозволяє отримати відповіді на наступні питання:

1) Які ризики в даний момент загрожують нашим бізнес-процесам?

2) На якому напрямку інформаційної безпеки потрібно зосередити увагу?

3) Скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації?

Оцінка ризику кількісно визначає чи якісно описує ризики і дає можливість керівникам розставляти ризики відповідно до пріоритетів згідно з пріоритетами серйозності або іншим встановленим критеріям [20].

Якісна / кількісна оцінка ризику (див. підрозділи. 3.1, 3.2)

Критерії:

- вартість збитку;
- собівартість продукції;
- очікування акціонерів.

Ризик-менеджмент включає в себе аналіз і оцінку сильних і слабких сторін організації з точки зору взаємодії з різними контрагентами (рис. 3.47).

Таблиця 3.40. Зведені дані дослідження БД уразливостей

БД	Критерії									
	Оцінка ризику/ ризик-калькулятор	Версії CVSS		Калькулятор CVSS		CVE ідентифікатор	CWE категорія	Можливість розширення	Вивід критичних загроз/ уразливостей	Можливість інтеграції
		v2.0	v3.0	v2.0	v3.0					
NVD	-	+	+	+	+	+	+	+	-	+
БДЗБІ	-	+	-	+	-	+	+	+	-	-
OSVDB	-	+	-	-	-	+	-	-	-	+
IBM X-Force	-	+	+	-	-	+	+	+	-	+
VND	-	+	+	-	-	+	+	+	+	+
Security Focus	-	-	-	-	-	+	-	+	-	+

Наведені критерії можуть бути корисними розробникам систем оцінювання ІБ. Також варто відзначити, що процедура оцінювання ризику не передбачена ні в одній із представлених БД.

Таким чином, визначено набір критеріїв для БД уразливостей PIC, за якими можна здійснити порівняльний аналіз таких баз і вибрати найбільш вдалі для побудови різних засобів оцінювання стану ІБ, наприклад, систем оцінювання ризиків або ризик-калькуляторів.

3.4. Оцінювання ризиків інформаційної безпеки

Організація повинна визначити та застосовувати процес оцінювання ризиків ІБ, який:

а) встановлює та підтримує критерії ризиків ІБ, які містять:

1) критерії прийняття ризиків;

2) критерії для виконання оцінки ІБ;

б) гарантує, що повторні оцінювання ризиків ІБ призводять до послідовних, дійових та порівняльних результатів;

в) ідентифікує ризики ІБ (см. рис. 3.47):

1) застосовує процес оцінювання ризиків ІБ для ідентифікації ризиків, пов'язаних із втратою конфіденційності, цілісності й доступності в межах сфери застосування СМІБ;

2) ідентифікує власників ризиків;

г) виконує аналіз ризиків ІБ:

1) оцінює потенційні наслідки, які будуть результатом реалізації ризиків, ідентифікованих в п. в) 1);

2) оцінює практичну імовірність появи ризиків, ідентифікованих у п. в) 1);

Згідно зі встановленими правилами, для кожної уразливості присвоюється CWE категорія, у відповідність з якою здійснюється їх групування за певними категоріями, що відображає так звані слабкі місця PIC. Наприклад, як показано на рис. 3.27, розглянутій уразливості присвоєна категорія CWE-17, а на рис. 3.33 відображено опис цього коду. Відповідно до представленого на сайті CWE™ звіту на 07.12.2015 р., зафіксовано 1004 CWE категорій слабких місць [66].

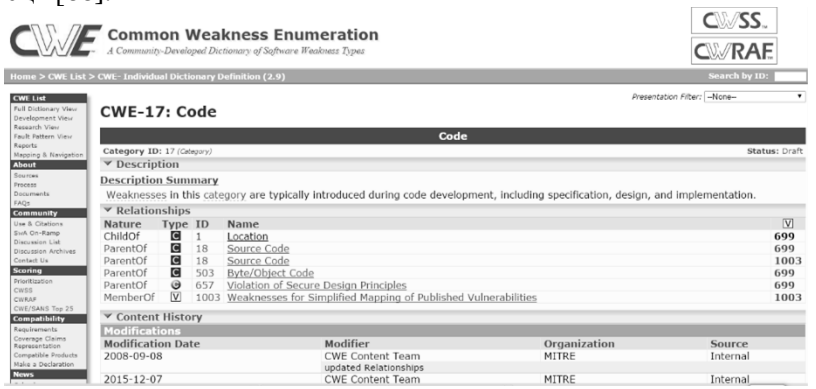


Рис. 3.33. Опис категорії CWE-17

Розглянемо приклади отримання значень з уразливості CVE-2015-1098 (Apple i Work Denial of Service Vulnerability) за допомогою CVSS v2.0 та CVSS v3.0 (див. табл. 3.37) [64].

Таблиця 3.37. Приклад обчислення CVSS

Показник		Значення показника		Числове значення	
v2.0	v3.0	v2.0	v3.0	v2.0	v3.0
AV		N	L	1	0,55
AC		M	L	0,61	0,44
Au	PR	N	N	0,704	0,27
-	UI	-	R	-	0,62
-	S	-	U	-	-
C		P	H	0,275	0,56
I		P	H	0,275	0,56
A		P	H	0,275	0,56
Результати CVSS для базової МГ				6,8	7.8

Приклад опису уразливостей, доступних для скачування в БД NVD, показаний в таблиці 3.38. Тут відображено уразливості з ідентифікаторами CVE-2015-0001 – «Windows Error Report-ing Security Feature Bypass Vulnerability» та CVE-2015-0032 – «VBScript Memory Corruption Vulnerability».

У представленій таблиці кожному стовпцю присвоєно номер, який відображає, наприклад, наступну інформацію про уразливість в БД:

1 – версія бази даних;

2 – дата публікації;

3 – ідентифікатор загрози;

Таблиця 3.38. Приклад опису уразливості

nvd_xml_version	pub_date	id	id2	operator	negate	name	operator3	negate4	name5	ns3:product	ns3:cve-id	ns3:published-datetime
1	2	3	4	5	6	7	8	9	10	11	12	13
2	09.12.2015 3:00:00	CVE-2015-0001	http://nvd.nist.gov/	OR	False	cpe:/o:microsoft:windows_8:-	-	-	-	cpe:/o:microsoft:windows_server 2012:r2:gold:-	CVE-2015-0001	2015-01-13T17:59:00.050-05:00
2	09.12.2015 3:00:00	CVE-2015-0032	http://nvd.nist.gov/	AND	False	-	OR	False	cpe:/a:microsoft:vbscript:5.6	cpe:/a:microsoft:vbscript:5.7	CVE-2015-0032	2015-03-11T06:59:01.290-04:00
2	09.12.2015 3:00:00	CVE-2015-0032	http://nvd.nist.gov	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-09-10T11:58:19.313-04:00	2015-09-10T11:58:19.313-04:00
1	09.12.2015 3:00:00	CVE-2015-0001	http://www.nist.gov/	OR	False	cpe:/o:microsoft:windows_8:-	-	-	-	cpe:/o:microsoft:windows_server 2012:r2:gold:-	CVE-2015-0001	2015-01-13T17:59:00.050-05:00

ns3:last-modified-datetime	ns4:score	ns4:access-vector	ns4:access-complexity	ns4:authentication	ns4:confidentiality-impact	ns4:integrity-impact	ns4:availability-impact	ns4:source	ns4:generated-on-datetime	id6	ns2:lang	reference_type	ns3:source	ns3:reference	Href	ns2:lang7	ns3:summary	ns3:security-protection
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2015-01-14T16:50:51.080-05:00	6,9	LOCAL	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-10-30T13:42:24.787-04:00	CWE-264	en	VENDOR_ADVISORY	MS	MS15-006	http://technet.microsoft.com/security/bulletin/MS15-006	en	*1)	-
2015-09-10T11:58:19.313-04:00	9,3	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-09-10T10:43:58.757-04:00	CWE-399	en	VENDOR_ADVISORY	MS	MS15-019	http://technet.microsoft.com/security/bulletin/MS15-019	en	*2)	-
2015-01-14T16:50:51.080-05:00	6,9	LOCAL	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-10-30T13:42:24.787-04:00	CWE-264	en	VENDOR_ADVISORY	MS	MS15-006	http://technet.microsoft.com/security/bulletin/MS15-006	en	*1)	-

* 1) Компонент звіту про помилки Windows (WER) в Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold, R2 і Windows RT Gold дозволяє локальним користувачам обійти механізм захисту і прочитати вміст в довільних місцях процесу-пам'яті за рахунок використання адміністративних привілеїв.

* 2) vbscript.dll в Microsoft VBScript 5.6 ÷ 5.8, який використовується з Internet Explorer 8 ÷ 11 та інших продуктах, дозволяє віддаленому зловмисникові виконати довільний код або викликати відмову в обслуговуванні (пошкодження пам'яті) за допомогою створеного Веб-сайту.

11 – назва продукту;

12 – CVE-ідентифікатор загрози;

14 – дата останньої зміни;

15 – оцінка CVSS (див. рис. 3.34);

16 – вектор доступу;

таблицю 3.40), за якими можна реалізовувати порівняння подібних БД.

До таких критеріїв належить наявність:

- оцінки CVSS за v2.0 і/або v3.0;
- калькулятора CVSS;
- ідентифікатора CVE;
- CWE категорії;
- можливості розширення;
- виведення критичних загроз/уразливостей;
- можливості інтеграції;
- оцінки ризику/ризик-калькулятора.

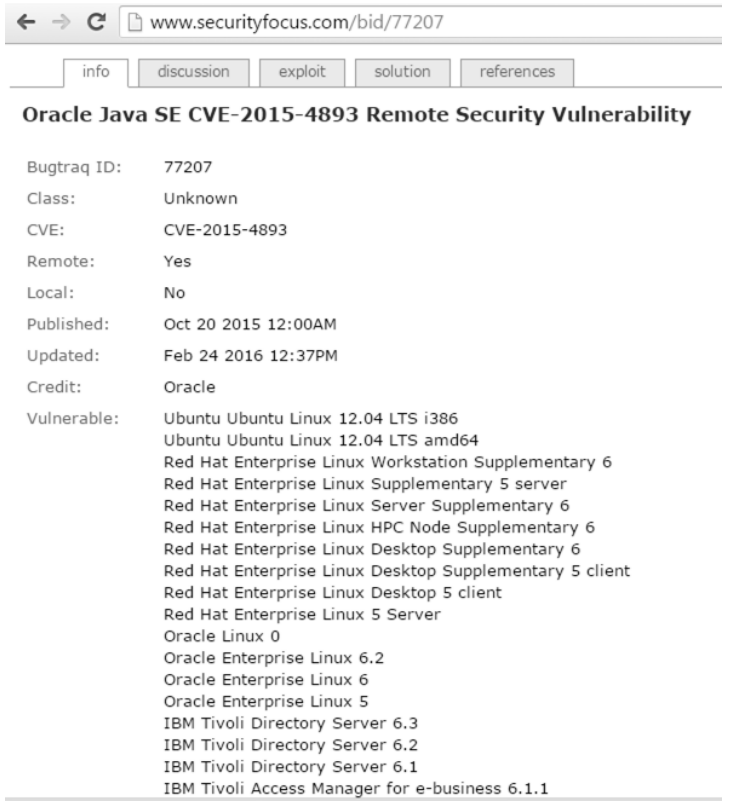


Рис. 3.46. Фрагмент вікна з прикладом опису уразливості Bugtraq 77270

На відміну від інших БД, уразливості фіксуються із зазначенням постраждалої сторони та інформації про продавця. Також на сайті БД VND присутня можливість отримання зведених даних оцінок CVSS уразливостей (див. рис. 3.44) [61].

База даних уразливостей SecurityFocus

База БД уразливостей SecurityFocus розроблена в 1999 та належить компанії Symantec (рис. 3.45) [62]. У SecurityFocus при додаванні уразливості останній присвоюється Bugtraq ID і визначається клас (рис. 3.46).

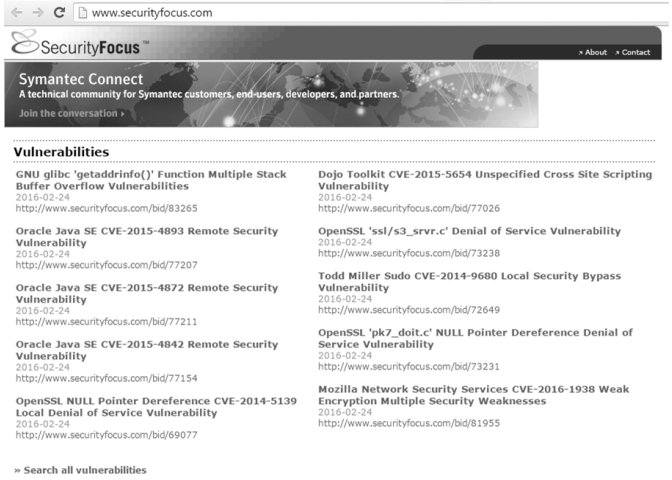


Рис. 3.45. Основна сторінка БД SecurityFocus

За аналогією з іншими відкритими БД уразливість також має:

- свій ідентифікатор CVE;
- дату опублікування і оновлення;
- інформацію про віддаленість або локальність;
- інформацію про уразливі продукти;
- обговорення (опис);
- інформація про використання;
- рішення про контрзаходи та рекомендації (див. рис. 3.46).

В результаті проведеного дослідження БД можна зробити висновки, що практично кожній уразливості, яка вноситься в ту чи іншу базу, присвоюється ідентифікатор CVE і визначається оцінка CVSS. Також під час дослідження було визначено критерії (див.

17 – складність доступу;

18 – аутентифікація;

19, 20, 21 – відповідно вплив на конфіденційність, цілісність та доступність;

22 – джерело;

23 – час появи;

24 – CWE категорія;

25 – мова;

26 – тип посилання;

30 – мова (опис щодо заданої адреси);

31 – резюме та ін. (див. табл. 3.38).

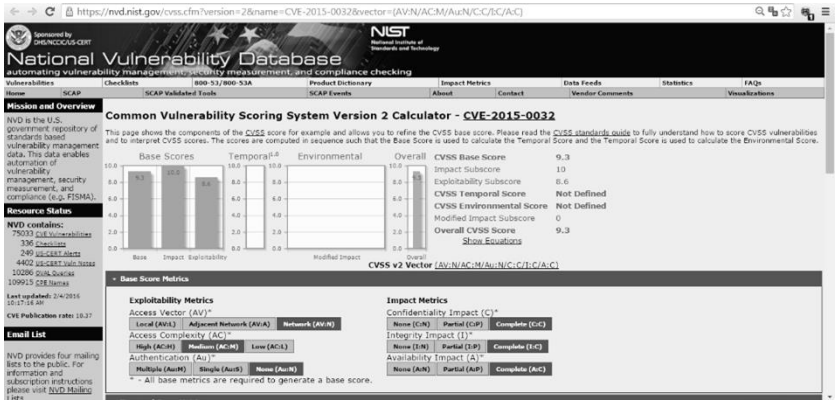


Рис. 3.34. Оцінка CVSS для CVE-2015-0032

Під час дослідження бази NVD було встановлено, що 82,77% уразливостей належать додаткам, 12,28% – ОС, а 3,59% – апаратному забезпеченню [53].

Банк даних загроз безпеки інформації

Банк даних загроз безпеки інформації (БДЗБІ) розроблений Федеральною службою з технічного та експортного контролю Росії та Державним науково-дослідним випробувальним інститутом проблем технічного ЗІ Росії.

Банк містить відомості про основні загрози та уразливості ІБ, у першу чергу, характерних для державних ІС та АС управління виробничими та технологічними процесами об'єктів критичних інфраструктур.

Відомості про загрози ІБ та уразливості ПЗ, що містяться в БДЗБІ, не є вичерпними і можуть бути доповнені за результатами аналізу відповідних загроз та уразливостей в конкретній ІС з урахуванням особливостей її експлуатації. Дані, що містяться в БДЗБІ, не є елементами ієрархічної класифікаційної системи, а є узагальненим переліком основних загроз та уразливостей ІБ (див. рис. 3.35) потенційно небезпечних для ІС. Останнє оновлення БДЗБІ від 11.07.16 р містило 186 загроз та 14395 уразливостей [58].

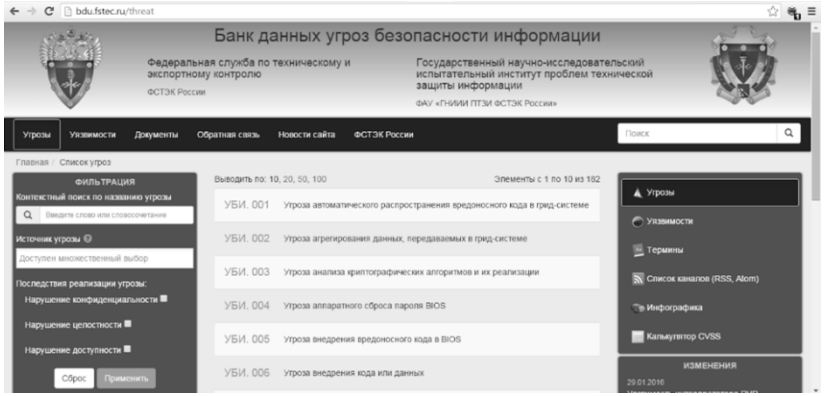


Рис. 3.35. Вікно сторінки опису загроз в БДЗБІ

Кожна загроза, яка вноситься до БДЗБІ, може бути описана наступними параметрами (рис. 3.35):

– унікальний ідентифікатор ЗБІ (загроза безпеці інформації);
– найменування загрози;
– опис загрози;
– джерело загрози (тип порушника та його мінімально необхідний функціонал (потенціал)) (див. рис. 3.36);
– об'єкт впливу;
– наслідки реалізації загрози [58].

У процесі внесення в БДЗБІ інформації про уразливість використовується наступний набір параметрів (див. рис. 3.37):

– ідентифікатор (складається з року та номеру за порядком);
– найменування уразливості;
– опис уразливості;

- https://flexerasoftware.flexnetoperations.com/control/inst/index
- http://securitymumblings.blogspot.com/2016/02/cve-2015-8277.html
- https://www.securifera.com/advisories/cve-2015-8277

Credit

Thanks to Matthew Benton, Ryan Wincey, and Richard Kelley for reporting this vulnerability.

This document was written by Joel Land.

Other Information

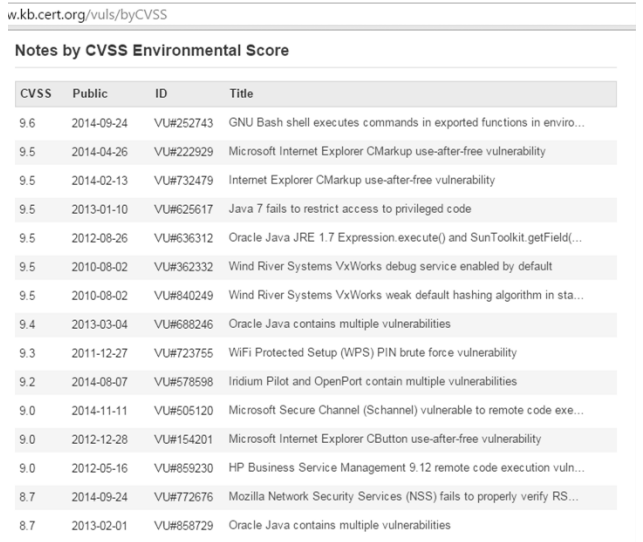
CVE IDs:	CVE-2015-8277
Date Public:	22 фев 2016
Date First Published:	22 фев 2016
Date Last Updated:	23 фев 2016
Document Revision:	22

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.

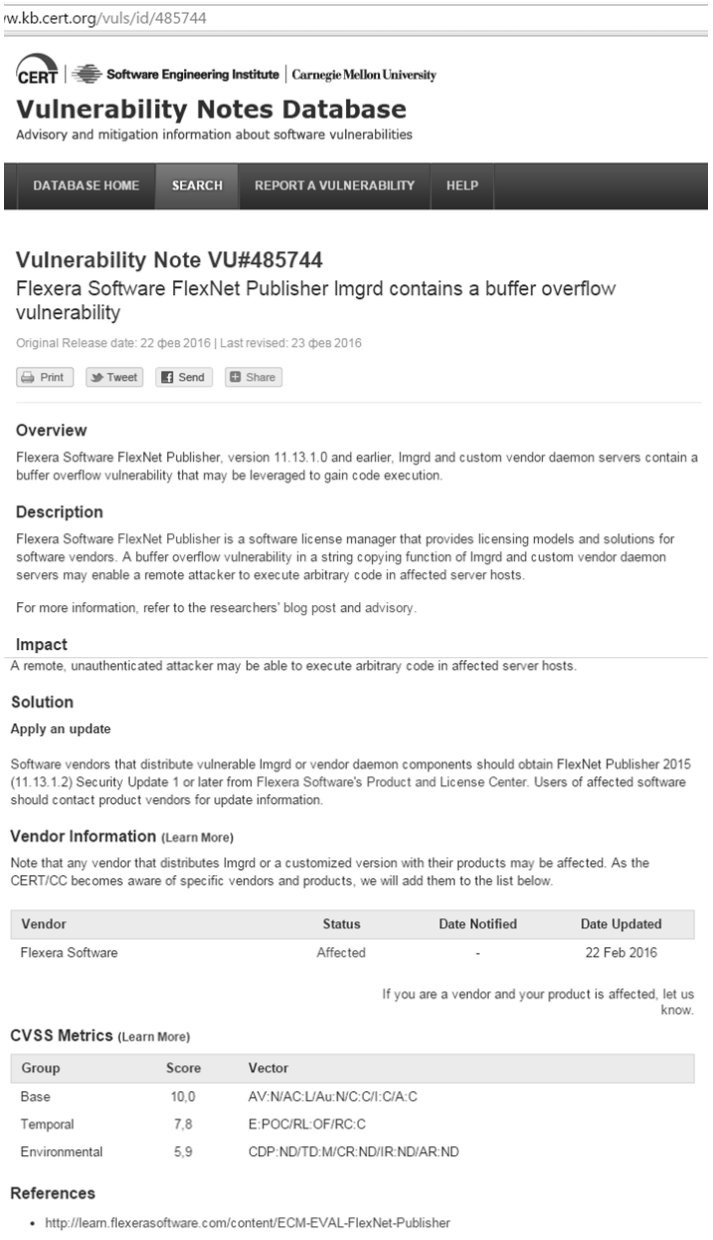
Рис. 3.43. Приклад опису уразливості

– рекомендації про усунення;
– оцінки CVSS;
– в додатковій інформації вказується (якщо є) ідентифікатор CVE;
– дата першої публікації та оновлення (див. рис. 3.44).



CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField(...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...
9.4	2013-03-04	VU#688246	Oracle Java contains multiple vulnerabilities
9.3	2011-12-27	VU#723755	WiFi Protected Setup (WPS) PIN brute force vulnerability
9.2	2014-08-07	VU#578598	Iridium Pilot and OpenPort contain multiple vulnerabilities
9.0	2014-11-11	VU#505120	Microsoft Secure Channel (Schannel) vulnerable to remote code exe...
9.0	2012-12-28	VU#154201	Microsoft Internet Explorer CButton use-after-free vulnerability
9.0	2012-05-16	VU#859230	HP Business Service Management 9.12 remote code execution vuln...
8.7	2014-09-24	VU#772676	Mozilla Network Security Services (NSS) fails to properly verify RS...
8.7	2013-02-01	VU#858729	Oracle Java contains multiple vulnerabilities

Рис. 3.44. Вільні дані оцінок CVSS



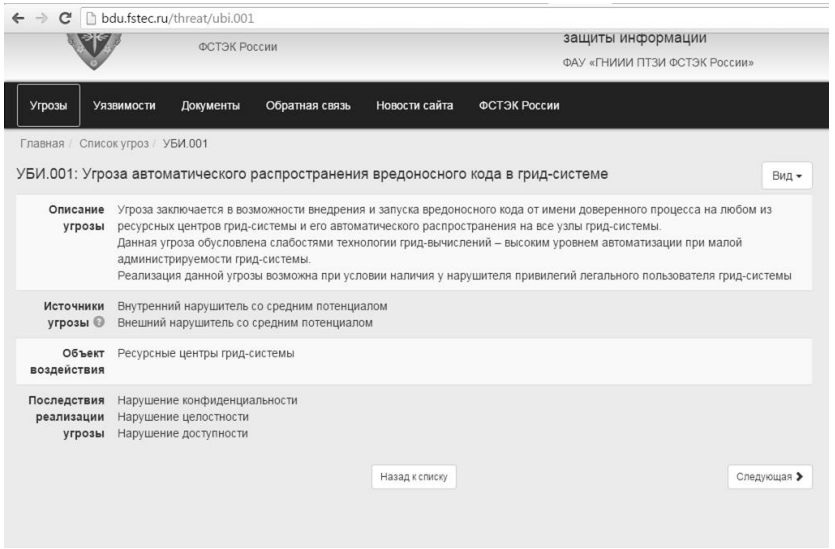
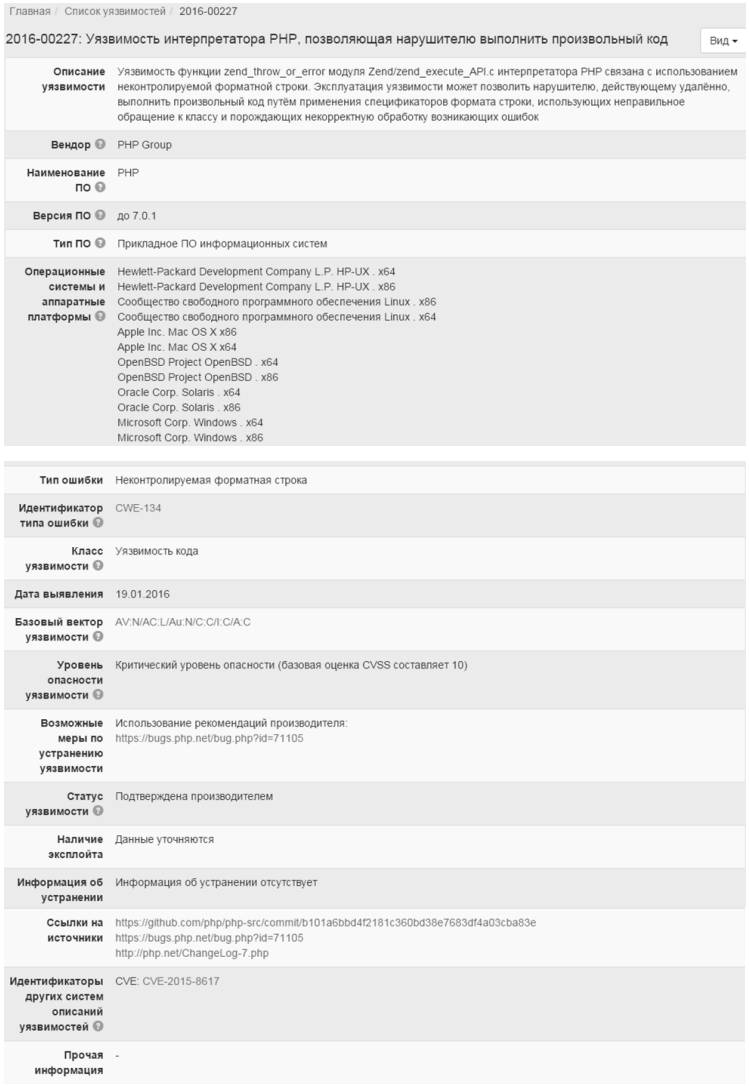


Рис. 3.36. Приклад опису ЗБІ: 001

– вендор (компанія – виробник ПЗ, в якому виявлена уразливість);
– назва ПЗ;
– версія ПЗ;
– тип ПЗ;
– ОС і апаратні платформи;
– тип помилки;
– ідентифікатор типу помилки (ідентифікатор, встановлений відповідно до загального переліку помилок CWE);
– клас уразливості;
– дата виявлення;
– вектор уразливості базової МГ (за CVSS v2.0);
– рівень небезпеки уразливості (за CVSS v2.0);
– можливі заходи щодо усунення уразливості;
– статус уразливості;
– наявність експлойта;
– інформація про усунення;
– посилання на джерела;

– ідентифікатори інших систем описів уразливостей (наприклад, CVE);
– інша інформація [58] (див. табл. 3.39).



Главная / Список уязвимостей / 2016-00227

2016-00227: Уязвимость интерпретатора PHP, позволяющая нарушителю выполнить произвольный код — Вид

Описание уязвимости	Уязвимость функции zend_throw_or_error модуля Zend/zend_execute_API.c интерпретатора PHP связана с использованием неконтролируемой форматной строки. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код путём применения спецификаторов формата строки, использующих неправильное обращение к классу и порождающих некорректную обработку возникающих ошибок
Вендор	PHP Group
Наименование ПО	PHP
Версия ПО	до 7.0.1
Тип ПО	Прикладное ПО информационных систем
Операционные системы и аппаратные платформы	Hewlett-Packard Development Company L.P. HP-UX . x64 Hewlett-Packard Development Company L.P. HP-UX . x86 Сообщество свободного программного обеспечения Linux . x86 Сообщество свободного программного обеспечения Linux . x64 Apple Inc. Mac OS X x86 Apple Inc. Mac OS X x64 OpenBSD Project OpenBSD . x64 OpenBSD Project OpenBSD . x86 Oracle Corp. Solaris . x64 Oracle Corp. Solaris . x86 Microsoft Corp. Windows . x64 Microsoft Corp. Windows . x86
Тип ошибки	Неконтролируемая форматная строка
Идентификатор типа ошибки	CWE-134
Класс уязвимости	Уязвимость кода
Дата выявления	19.01.2016
Базовый вектор уязвимости	AV:N/AC:L/Au:N/C:C/I:C/A:C
Уровень опасности уязвимости	Критический уровень опасности (базовая оценка CVSS составляет 10)
Возможные меры по устранению уязвимости	Использование рекомендаций производителя: https://bugs.php.net/bug.php?id=71105
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Данные уточняются
Информация об устранении	Информация об устранении отсутствует
Ссылки на источники	https://github.com/php/php-src/commit/b101a6bbd4f2181c360bd38e7683df4a03cba83e https://bugs.php.net/bug.php?id=71105 http://php.net/ChangeLog-7.php
Идентификаторы других систем описаний уязвимостей	CVE: CVE-2015-8617
Прочая информация	-

Рис. 3.37. Фрагмент прикладу опису уразливості 2016-00227 в БДЗБІ

Як видно з опису уразливості на рис. 3.41, використовуються за аналогією з попередніми базами оцінки CVSS (до 2016 року використовувалася v2.0, після – v3.0), ідентифікатор CVE, короткий опис, дата створення звіту про уразливість, задіяних продуктів, в яких є ця уразливість і зовнішні посилання.

Але, на відміну від інших БД, тут присутнє поле «Наслідки», що виражає в формалізованому вигляді можливий результат експлуатації уразливості, наприклад, «Gain Access» (отримання доступу) та «Виправлення», де наведені варіанти контрзаходів [53, 60].

База даних записів уразливостей US-CERT

База БД VND (див. рис. 3.42) записів уразливостей US-CERT належить United States Computer Emergency Readiness Team (US-CERT). Вона розроблена спільно з Office of Cybersecurity and Communications (Управління кібербезпеки і комунікацій), Department of Homeland Security (Департамент внутрішньої безпеки), Software Engineering Institute (інженерний інститут ПЗ) та Carnegie Mellon University (інститут Карнегі-Мелоуна).

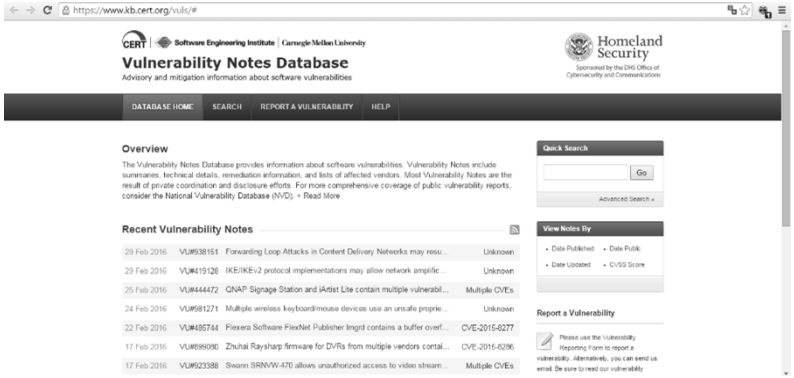


Рис. 3.42. Основна сторінка VND

Кожній уразливості в БД присвоюється свій ідентифікатор «VU #», як показано на рис. 3.43 (VU # 485744).

За аналогією з розглянутими вище БД, в VND наявні такі наступні основні пункти опису уразливості:

– огляд;
– короткий опис;
– вплив;

База даних уразливостей IBM X-Force

База БД уразливостей IBM ISS (Internet Security Services) X-Force, створена фахівцями підрозділу IBM Internet Security Systems X-Force, є однією з найбільших та авторитетних БД в галузі. Вона містить понад 30000 записів і детальний аналіз кожної відомої уразливості, виявленої з 1994 року.

Більш того, фахівці підрозділу X-Force співпрацюють з тисячами найбільших в світі компаній та державних установ, центрами аналізу і вертикального обміну інформацією (ISAC), глобальними координаційними центрами та іншими постачальниками рішень [67]. Для доступу до БД уразливостей необхідно пройти реєстрацію на сайті IBM X-Force Exchange. Після реєстрації в рядку пошуку необхідно задати потрібну інформацію про уразливість (див. рис. 3.41).

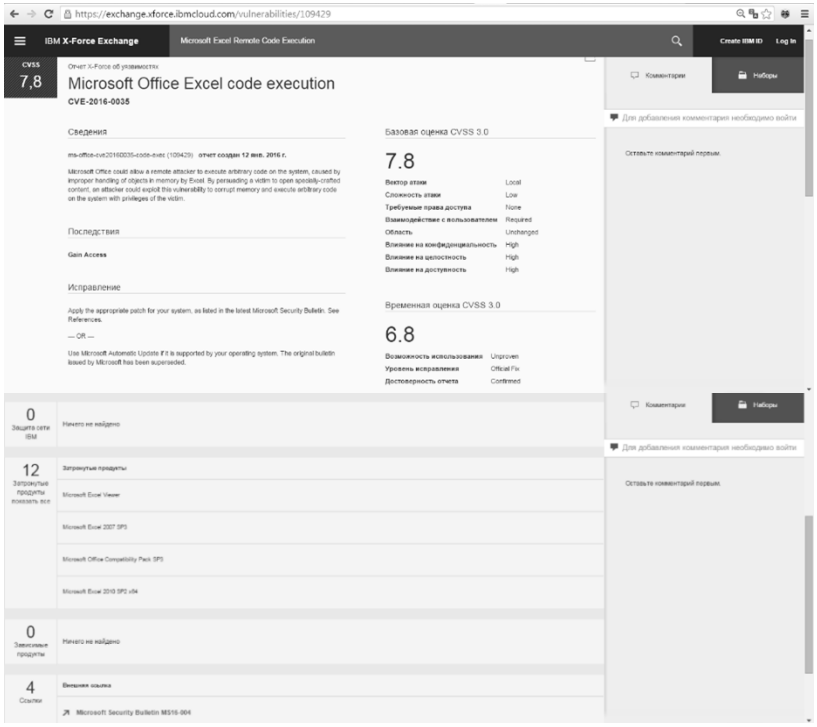


Рис. 3.41. Приклад опису уразливості Microsoft Excel Remote Code Execution

Таблиця 3.39. Приклад звіту уразливостей

№п/п	Найменування уразливості	Відкритий ідентифікатор уразливості	Ідентифікатори інших систем описів уразливостей	Опис уразливості	Назва ПЗ	Версія ПЗ	Клас уразливості	Назва ОС і тип апаратної платформи	Дата виявлення	Базовий вектор CVSS	Рівень небезпеки уразливості	Можливі заходи з усунення	Статус уразливості	Наявність експлойта	Інформація про усунення	Посилання на джерело	Вендор ПЗ	Інша інформація	Опис помилки CWE	Тип помилки CWE
1	Уразливість вбудованого ПЗ програмованого логічного контролера Schneider Electric Modicon Quantum, що дозволяє зловмисникові отримати авторизований доступ до пристрою	2014-00001	CVE-2011-4859	Мікропрограмне забезпечення модуля 140NOE77111 контролера Schneider Electric Modicon Quantum містить множинну пар логін: пароль, встановлених за замовчуванням. Це дозволяє будь-якому користувачеві, що має доступ до пристрою по протоколу FTP, отримати авторизований доступ до пристрою	Мікропрограмне забезпечення програмованого логічного контролера Schneider Electric Modicon Quantum	4.6	Уразливість архітектури	Мікропрограмне забезпечення програмованого логічного контролера Schneider Electric Modicon Quantum (4.6)	17.12.2011	AV:N/AC:L/Au:N/C:C/I:C/A:C	Критичний рівень небезпеки (базова оцінка CVSS становить 10)	Обмеження доступу до пристрою за протоколом FTP	Підтверджено виробником	Існує	Інформація про усунення відсутня	http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-020-03	Schneider Electric	Мова розробки ПЗ – C	Жорстке кодування паролів	CWE-259	

Також на сайті БДЗБІ міститься калькулятор CVSS v2.0 (див. рис. 3.38), що є русифікованою версією аналогічного калькулятора NVD. Тут представлена і інфографіка, на якій відображені зведені дані за різними параметрами (рис. 3.39).

Open Sourced Vulnerability Database

Open Sourced Vulnerability Database (OSVDB). База створена OSVDB в 2002 році як незалежна та відкрита БД уразливостей для фахівців в області ІБ. Мета проекту полягала в тому, щоб забезпечити точну, деталізовану та актуальну інформацію про уразливості для систем забезпечення ІБ [53]. Станом на 5 травня 2014 року дана база містила 105413 уразливостей. Веб-інтерфейс OSVDB (див. рис. 3.40) не надто відрізняється від бази NVD.

Кожна уразливість, що заноситься в OSVDB, описується наступним чином:

- ідентифікатор OSVDB;
- дата виявлення;
- ім'я виробника;

– ім'я продукту;

– версія продукту (символьне значення), що має дану уразливість;

– посилання, яке вказує на пряму адресу інтернет-ресурсу іншої бази або бази виробника, в якій описується дана уразливість;

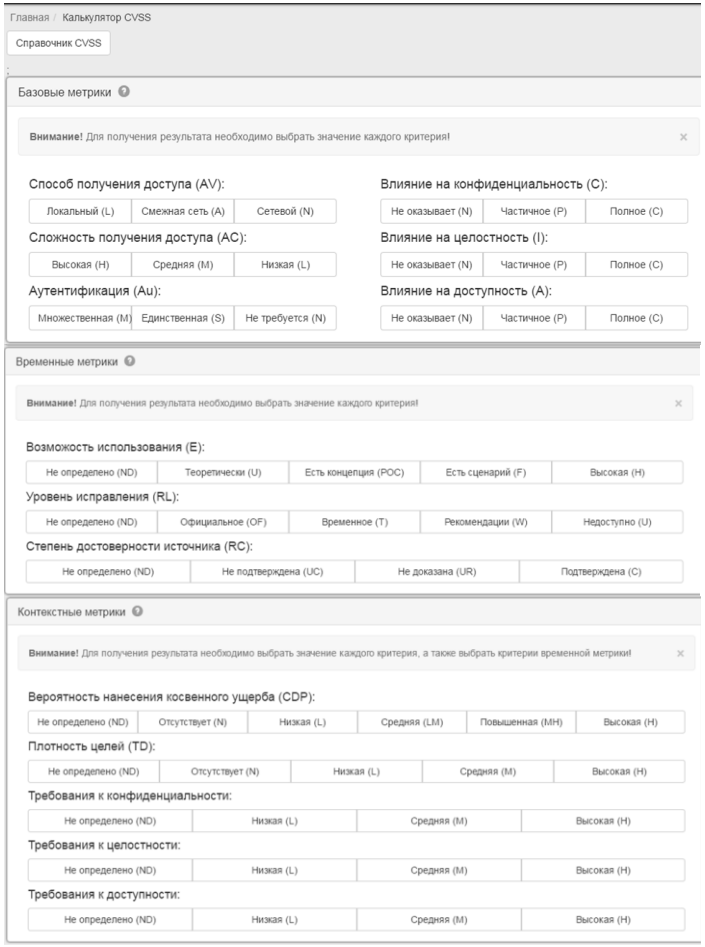


Рис. 3.38. Інтерфейс калькулятора CVSS v2.0 на сайті БДЗБІ

– рішення, яке має опис «виправлення» уразливості;

– метрики уразливості, що містять критерії оцінки уразливостей в форматі CVSS v2.0 (не є обов'язковими з огляду на те, що поле є присутнім при наявності посилання на базу NVD) [53, 59].

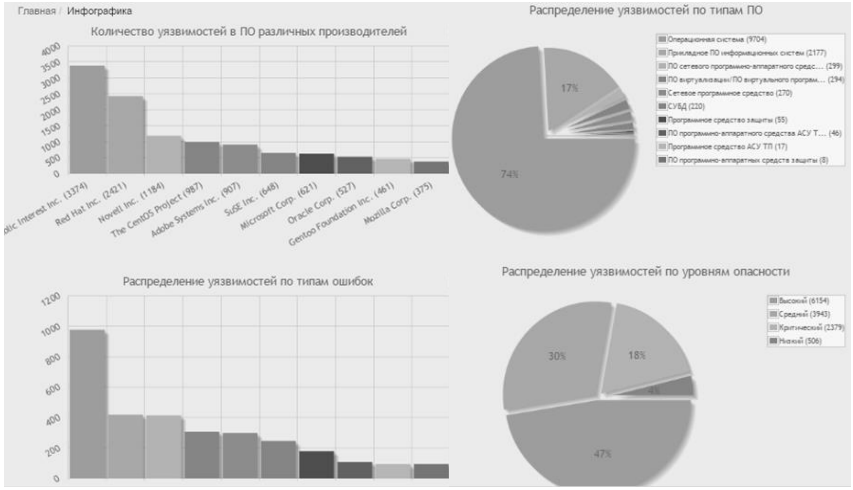


Рис. 3.39. Інфографіка БДЗБІ

Варто відзначити, що OSVDB з 2016 року стала умовно відкритою БД і тепер надаються платні послуги за інформацією про уразливості. При цьому, її розробники уклали договір із співпраці з компанією Risk Based Security, яка продає клієнтам ліцензії на отримання доступу до даних.

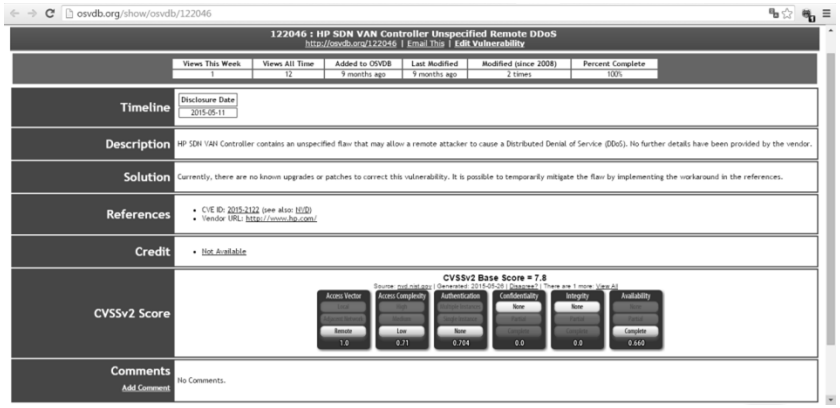


Рис. 3.40. Інтерфейс OSVDB