МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
Кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Інциденти інформаційної безпеки. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 62 с.

Укладачі: ГРЕБЕННИК АЛЛА ГРИГОРІВНА, старший викладач кафедри кібербезпеки та математичного моделювання;
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор;
СЕМЕНДЯЙ СЕРГІЙ МАТВІЙОВИЧ, старший викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ,
професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор

ЗМІСТ

ВСТУП

Методичні вказівки до виконання лабораторних робіт призначені для підготовки та виконання лабораторних робіт з дисципліни «Інциденти інформаційної безпеки» для студентів спеціальності 125 «Кібербезпека та захист інформації».

Основна мета дисципліни «Інциденти інформаційної безпеки» полягає у отриманні студентами необхідних знань щодо моніторингу, розробки та впровадження системи управління інцидентами інформаційної безпеки, що включає процеси, нормативно-розпорядчу документацію і засоби автоматизації.

У методичних вказівках наведено: необхідні теоретичні відомості, практичні завдання, які повинен виконати студент, та теоретичні запитання, відповіді на які повинен знати студент. Вміщено також перелік рекомендованої літератури.

При підготовці до виконання лабораторної роботи студент повинен вивчити відповідні теоретичні відомості, передбачені навчальною програмою, ознайомитись із завданням лабораторної роботи. Після закінчення кожної роботи студенти складають індивідуальні звіти, що містять теоретичні відомості, результати роботи з необхідними матеріалами і коментарями, висновки по роботі. Під час захисту лабораторних робіт студент повинен показати знання відповідних розділів курсу, методів розв’язання практичних завдань та досліджень, виконаних у роботі.

Лабораторна робота № 1

Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами інформаційної безпеки

Мета роботи – проаналізувати особливості законодавства України та стандартів ISO/IEC в частині управління інцидентами інформаційної безпеки, навчитись застосовувати вимоги стандартів та нормативних документів до систем управління інцидентами інформаційної безпеки.

Теоретичні відомості

Міжнародна нормативно-методологічна база з керування інцидентами інформаційної безпеки.

У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі інформаційної безпеки (ІБ) проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам ІБ на різних стадіях узгодження і затвердження.

Розробка нормативних документів з ІБ, повністю або частково присвячених керуванню інцидентами ІБ, здійснюється спеціалізованими міжнародними організаціями і консорціумами, наприклад такими як: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open тощо. Значна робота щодо стандартизації питань ІБ, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST, CMU/SEI; Німеччині та Великобританії – BSI. Все це дозволило сформувати широку нормативно-методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами ІБ. Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO.

Стандарти ISO серій 9000, 27002, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, за основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти зазначених серій використовують єдину модель PDCA як структуру життєвого циклу всіх процесів системи менеджменту.

Основні нормативно-методологічні документи ISO/IEC, що за певними аспектами регламентують процеси керування інцидентами ІБ, наведені в таблиці 1.1.

Таблиця 1.1 – Нормативно-методологічні документи ISO/IEC, що стосуються керування інцидентами ІБ

№ п/п	Позначення документу	Назва документу
1	ISO/IEC 27002	Information technology. Security techniques. Code of practice for information security management Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки
2	ISO/IEC 27001	Information technology. Security techniques. Information security management systems. Requirements. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги
3	ISO/IEC 27035	Information technology. Security techniques. Information security incident management. Методи захисту. Керування інцидентами інформаційної безпеки.
4	ISO/IEC 20000	ISO/IEC 20000-2:2012. Information technology. Service management. Part 2: Code of practice. Інформаційні технології. Менеджмент послуг. Частина 2. Настанова щодо застосування систем управління послугами

Як свідчить світова практика стандарт **ISO/IEC 27002** [1] на сьогодні став найпоширенішим інструментом створення системи керування інформаційною безпекою (СКІБ), стандартом де-факто щодо керування ІБ. Стандарт розроблений в 2005 році на основі версії ISO 17799, опублікованій у 2000. Відмітимо, що остання версія офіційно прийнята в Україні як ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT) 17.08.2023р.

ISO/IEC 27002– це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування ІБ, а також загальні принципи побудови системи керування ІБ. В цьому ж документі визначено такі базові терміни, як:

подія інформаційної безпеки - ідентифікований стан системи, служби або мережі, що вказує на можливе порушення політики інформаційної безпеки чи відмову засобів захисту або раніше невідому ситуацію, яка може мати відношення до безпеки [1, п. 2.6].

інцидент інформаційної безпеки - на інцидент інформаційної безпеки вказує одна або серія небажаних або непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації функціонування бізнесу і загрози інформаційній безпеці [1, п. 2.7].

Розділ 13 ISO/IEC 27002 присвячено керуванню інцидентами ІБ. В ньому розглянуто наступні питання.

Звітування щодо подій та слабких місць ІБ [1, п. 13.1]. Виявлення користувачами подій і слабких місць ІБ, пов'язаних з інформаційними системами, має гарантувати можливість ухвалення своєчасних корегуючих дій. Має бути впроваджений формальний порядок звітування про події і порядок ескалації. Всіх співробітників, контрагентів і користувачів третіх сторін слід поінформувати про порядок повідомлення щодо різних типів подій і слабких місць, які можуть мати вплив на безпеку активів організації. Дані особи зобов'язані негайно повідомляти про будь-які події і слабкі місця ІБ, використовуючи певну точку контакту. Про події ІБ потрібно повідомляти за допомогою прийнятних каналів керування настільки швидко, наскільки це можливо.

Разом з формальним порядком повідомлення про події ІБ, слід затвердити і порядок реагування на інциденти або ескалації. В цих порядках потрібно описати дії, що мають бути здійснені при отриманні повідомлення про подію ІБ. Слід встановити точку контакту для повідомлень про події ІБ. Слід забезпечити обізнаність всієї організації про дану точку контакту, її постійну доступність і здатність адекватно і своєчасно реагувати.

Порядок повідомлення має включати:

– відповідні процедури зворотного зв’язку для забезпечення того, щоб особи, які звітували про подію інформаційної безпеки, були сповіщені про результати після того, як проблему було оброблено й закрито;
– форми звітування про подію інформаційної безпеки для підтримування звітування і допомоги особі, що звітує, запам’ятати всі необхідні дії у разі події інформаційної безпеки;
– правильну поведінку у разі події ІБ, тобто: негайний запис всіх важливих подробиць (наприклад, тип невідповідності або порушення, збій, повідомлення на екрані, дивна поведінка); не виконувати будь-яких самостійних дій, а негайно повідомити в точку контакту;
– посилання на офіційно оформлений дисциплінарний процес вживання заходів до співробітників, контрагентів або користувачів, третіх сторін, що здійснили порушення безпеки.

Прикладами подій та інцидентів інформаційної безпеки є:

a) втрата послуги, обладнання або засобів обслуговування;
b) збій або перевантаження системи;
c) людські помилки;
d) невідповідності політиці або настановам;

e) порушення заходів фізичної безпеки;
f) неконтрольовані зміни системи;
g) збій програмного забезпечення або апаратних засобів;
h) порушення доступу.

При належному дотриманні заходів щодо конфіденційності, інформацію про інциденти ІБ можна використовувати в тренінгах з підвищення поінформованості користувачів як приклади того, що може трапитися, як реагувати на такі інциденти і як уникати їх в майбутньому. Щоб бути здатними правильно враховувати події та інциденти інформаційної безпеки, може бути необхідним збирати докази якнайшвидше після того, як вони відбулися.

Збої або інша аномальна поведінка системи можуть свідчити про атаку на безпеку або фактичне порушення безпеки, тому слід завжди повідомляти про них, як про події ІБ.

Всіх співробітників, контрагентів і користувачів, третіх сторін, що використовують інформаційні системи і послуги, слід зобов'язати звертати увагу і повідомляти про будь-які помічені або передбачувані слабкі місця ІБ в системах або послугах. Механізм повідомлення повинен бути якомога легким та зручним. Слід проінформувати всіх, що ні за яких обставин не можна намагатися перевіряти і демонструвати передбачуване слабке місце.

Випробування слабких місць можна тлумачити як потенційне неправомірне використання системи, що може також привести до пошкоджень інформаційної системи або служби та до юридичної відповідальності особи, що виконує перевірку.

Керування інцидентами та вдосконаленням ІБ [1, п. 13.2]. Забезпечення застосування послідовного і ефективного підходу до керування інцидентами ІБ.

Повинні бути наявними відповідальності та процедури ефективної обробки подій та слабких місць інформаційної безпеки одразу ж після звітування про них. До реагування, моніторингу, оцінювання та загального управління інцидентами інформаційної безпеки повинен застосовуватися процес безперервного вдосконалення. Там, де потрібні докази, вони повинні бути зібрані, щоб забезпечити відповідність правовим вимогам.

Необхідно розглянути наступні рекомендації щодо порядку керування інцидентами ІБ:

– слід затвердити порядок поводження з різними типами інцидентів ІБ, включаючи: збої інформаційних систем; шкідливий код; відмову в обслуговуванні; помилки через неповні або неточні дані; порушення конфіденційності та цілісності; неправомірне використання інформаційних систем;
– на додаток до звичайних планів реагування для непередбачуваних обставин, порядок має також охоплювати: аналіз та ідентифікацію причин інциденту; обмеження розповсюдження; планування і впровадження корегуючих дій;

зв'язок з особами, відповідальними за процес відновлення після інциденту або задіяними в даний процес; повідомлення у відповідні державні органи;
- при необхідності, слід збирати і захищати протоколи (audit trails) та інші подібні докази;
- слід ретельно та формально керувати заходами щодо відновлення після порушень ІБ та виправлення збоїв системи порядок яких повинен забезпечувати: дозвіл доступу до виробничих чи технологічних систем і даних тільки чітко встановленому і уповноваженому персоналу; докладне документування всіх вжитих аварійних заходів; повідомлення керівництву про надзвичайні заходи і їх системний розгляд; підтвердження цілісності систем бізнесу та засобів керування з мінімальною затримкою.

Цілі управління інцидентами ІБ повинні бути погоджені з керівництвом, і треба забезпечити, щоб особи, відповідальні за управління інцидентами ІБ, розуміли пріоритети організації щодо обробки інцидентів інформаційної безпеки.

Інциденти ІБ можуть виходити за рамки організації і держави. Для реагування на такі інциденти зростає потреба в координації реагування та в обміні інформацією стосовно інцидентів із зовнішніми організаціями.

Вивчення інцидентів ІБ [1, п. 13.2.2]. Слід впровадити механізми, які дозволяють визначати кількість і здійснювати моніторинг типів, обсягів та вартості інцидентів ІБ. Інформація, отримана від оцінювання інцидентів, повинна використовуватися для ідентифікації інцидентів, які повторюються або мають великий вплив. Оцінка інцидентів ІБ може вказати на потребу в удосконалених або додаткових контролях з метою зниження частоти, ушкодження та вартості майбутніх проявів інцидентів, або взята до уваги в процесі перегляду політики безпеки.

Збір доказів [1, п. 13.2.3]. Якщо після інцидентів ІБ відносно людини або організації вживаються заходи, що передбачають судовий позов (цивільний або кримінальний), треба зібрати, зберегти та представляти докази згідно з правилами, щодо доказів, прийнятим у відповідній юрисдикції. Повинні бути розроблені і виконуватися внутрішні процедури збирання й надання доказів для дисциплінарних заходів, здійснюваних організацією. У загальному випадку правила щодо доказів охоплюють: a) припустимість доказу: може чи ні доказ бути використаний у суді; b) вагомість доказу: якість та повнота доказу. Щоб досягти припустимості доказу, організація має переконатися, що її інформаційні системи відповідають певному опублікованому стандарту або зведенню правил зі збору допустимих доказів, які можуть бути прийняті до розгляду судом.

Вагомість доказу, що надається, повинна задовольняти будь-які застосовні вимоги. Щоб досягти вагомості доказу, повинні бути продемонстровані в доказовому виді якість та повнота контролів, використовуваних для правильного та несуперечливого захисту доказу (тобто, доказ процесу контролю) протягом

періоду зберігання та оброблення доказу. Взагалі, така доказовість може бути встановлена за таких умов:

a) для паперових документів: оригінал надійно зберігають з реєстрацією особи, яка знайшла документ, де і коли цей документ було знайдено і хто був свідком знаходження; будь-яке розслідування повинне пересвідчитися, що оригінали не підроблені;

b) для інформації на комп'ютерних носіях: повинні братися дзеркальні відображення або копії (залежно від застосовних вимог) будь-якого змінного носія, інформації з жорстких дисків або пам'яті; повинен зберігатися журнал всіх дій протягом процесу копіювання і процес повинен бути проходити при свідках; оригінальний носій та журнал реєстрації (якщо це неможливо, то хоча б одне дзеркальне відображення або копія) повинні бути надійно збережені і недоторкані.

Будь-яку роботу з розслідування інциденту слід виконувати тільки на копіях доказового матеріалу. Цілісність усіх доказових матеріалів повинна бути захищена. Копіювання доказового матеріалу повинне здійснюватися під наглядом персоналу, який заслуговує довіри, з обов'язковою реєстрацією інформації: коли і де виконувався процес копіювання, хто здійснював копіювання і які інструменти та програми були використані.

Коли подію ІБ виявлено вперше, може не бути очевидним, чи дійсно ця подія призведе до судових дій. Тому існує небезпека, що необхідний доказ буде зруйнований навмисно або випадково до усвідомлення серйозності інциденту. Тому бажано завчасно в будь-яку правову діяльність залучити адвоката або поліцію і отримати рекомендації щодо необхідного доказу.

Докази можуть виходити за межі організації та/або юрисдикції. У таких випадках треба забезпечити, щоб організація мала право збирати необхідну інформацію як доказ. Щоб максимально збільшити можливості визнання за межами відповідної юрисдикції, повинні також бути розглянуті вимоги різних юрисдикцій.

Стандарт **ISO/IEC 27001** [2] створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління ІБ (СУІБ), що стосуються в тому числі і процесів керування інцидентами ІБ. Остання версія офіційно прийнята в Україні як ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT) 17.08.2023р.

Згідно з ISO/IEC 27001 для обробки подій і інцидентів ІБ необхідно організувати *процес* реагування на інциденти. Основними *завданнями* процесу реагування на інциденти ІБ є:

– координація реагування на інцидент ІБ;
– підтвердження / спростування факту виникнення інциденту ІБ;

– забезпечення збереження і цілісності доказів виникнення інциденту ІБ, створення умов для накопичення і зберігання точної інформації про інциденти ІБ, що мали місце, про корисні рекомендації;
– мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни працездатності компанії при її порушенні в результаті інциденту;
– мінімізація наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем;
– захист прав компанії, встановлених законом;
– створення умов для порушення цивільної або кримінальної справи проти зловмисників;
– захист репутації компанії і її ресурсів;
– швидке виявлення і/або попередження подібних інцидентів в майбутньому;
– навчання персоналу компанії діям щодо виявлення, усунення наслідків і запобігання інцидентам ІБ.

В рамках ISO/IEC 27001 висуваються наступні вимоги до процесу реагування на інциденти ІБ, які повністю відповідають вищерозглянутим *рекомендаціям* щодо керування інцидентами ІБ у ISO/IEC 27002:

Моніторинг, вимірювання, аналіз та оцінювання СКІБ [2, п. 9.1]. Організація повинна оцінювати результативність інформаційної безпеки, ефективність системи управління інформаційною безпекою та визначати:

a) що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки;

b) методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;

c) коли моніторинг та вимірювання потрібно виконувати;

d) хто повинен виконувати моніторинг та вимірювання;

e) коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати; та

f) хто повинен аналізувати й оцінювати ці результати.

Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

Управління інцидентами інформаційної безпеки [2; Додаток А.16].

А.16.1.1 *Відповідальності та процедури*. Має бути визначено відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти ІБ.

А.16.1.2 *Звітування про події ІБ*. Необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки через належні канали управління.

А.16.1.3 *Звітування щодо слабких місць ІБ.* Треба вимагати від усього найманого персоналу та підрядників, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких

спостережених або очікуваних слабких місць у системах чи сервісах.

А.16.1.4 *Оцінювання та прийняття рішення стосовно подій ІБ*. Події ІБ має бути оцінено та прийнято рішення стосовно віднесення їх до інцидентів інформаційної безпеки.

А.16.1.5 *Реагування на інциденти ІБ*. Реагування на інциденти ІБ має здійснюватися відповідно до задокументованої процедури.

А.16.1.6 *Знання з вивчення інцидентів ІБ*. Знання, отримані з аналізу та розв'язання інцидентів ІБ, мають використовуватися для зменшення ймовірності чи впливу майбутніх інцидентів.

А.16.1.7 *Збирання доказів*. Організація повинна визначити і використовувати процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази.

Задачам керування інцидентами ІБ присвячено стандарт **ISO/IEC 27035** [3]. Даний документ описує інфраструктуру керування інцидентами в рамках циклічної моделі PDCA. Стандарт представлено в трьох частинах, зокрема, ISO/IEC 27035-1:2016 «Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management», ISO/IEC 27035-2:2016 «Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response», а також ISO/IEC 27035-3:2020 Information technology «Information security incident management – Part 3: Guidelines for ICT incident response operations». В ньому відповідно перша частина стосується основних принципів управління інцидентами, друга містить настанови щодо планування та підготовки до реагування на інциденти, третя присвячена настановам щодо операцій з реагування на інциденти в ІКТ (інформаційно-комунікаційних технологіях).

Останні версії офіційно прийняті в Україні як ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT) та ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT) 10.12.2018р.

ISO/IEC 27035 визначає формальну модель процесу реагування на інциденти. *Цілями* проходження цієї моделі є упевненість в тому, що:

– події і інциденти ІБ виявляються і обробляються ефективним чином, особливо в частині класифікації;
– виявлені інциденти ІБ враховуються і обробляються найбільш відповідним і ефективним чином;
– наслідки інцидентів ІБ можуть бути мінімізовані в процесі реагування на інциденти ІБ, можливо із залученням процесів відновлення після збоїв і аварій (DRP/BCP);

– за рахунок аналізу інцидентів і подій ІБ підвищується вірогідність запобігання майбутнім інцидентам, поліпшуються механізми і процеси забезпечення ІБ.

Процес реагування на інциденти ІБ складається з наступних *етапів*:

Планування і підготовка. На даному етапі здійснюється розробка схеми реагування на інциденти ІБ, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація вибраної схеми реагування на інциденти ІБ. Даний етап є підготовчим і призначений для організації і регламентації діяльності з реагування на інциденти ІБ.

На цьому етапі необхідно:

– виділити людські і матеріальні ресурси;
– розробити схему реагування на інциденти ІБ;
– розробити і затвердити ряд організаційно-регламентуючих документів;
– провести необхідне навчання персоналу і апробацію вибраної схеми реагування на інциденти ІБ.

Відповідно до ISO/IEC 27035 необхідно створити групу з розслідування інцидентів ІБ. Основні цілі якої:

– забезпечення компанії кваліфікованим персоналом для обліку, реагування і аналізу інцидентів ІБ;
– забезпечення необхідної координації і керування процесом реагування на інциденти ІБ;
– забезпечення належного рівня інформування керівництва і зацікавлених осіб;
– забезпечення максимального зниження наслідків інцидентів ІБ як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи рекомендується включити представників наступних підрозділів організації:

– служба ІБ: забезпечення координаційної, адміністративної, експертної і технологічної діяльності;
– служба ІТ: забезпечення експертної і технологічної діяльності;
– служба персоналу: забезпечення адміністративної і процедурної діяльності;
– юридична служба: забезпечення експертної і нормативно-правої діяльності;
– бізнес-менеджери профільних підрозділів: притягуються на тимчасовій основі для підтримки забезпечення адміністративної, експертної і технологічної діяльності;
– зовнішні експерти: забезпечення консультативної, експертної і технологічної діяльності.

Основними процесами підготовчого етапу можуть бути:

– виділення людських і матеріальних ресурсів;
– розробка і затвердження організаційно-розпорядчої документації;
– навчання персоналу;
– тестування схеми реагування на інциденти ІБ.

Експлуатація. Здійснюється виявлення інциденту ІБ, його ідентифікація, попередній аналіз і початкове реагування.

Аналіз. Група з реагування на інциденти ІБ проводить поглиблений аналіз інциденту ІБ, на основі результатів аналізу робляться висновки і складаються рекомендації з поліпшення процесу забезпечення ІБ і реагування на інциденти. Формується звіт про інцидент ІБ. Основним процесом етапу є поглиблений аналіз інциденту ІБ.

Поліпшення. На даному етапі здійснюється реалізація рекомендацій щодо поліпшення процесів забезпечення ІБ і реагування на інцидент. Затверджені уповноваженою особою компанії рекомендації передаються на виконання відповідальним особам.

Необхідно відзначити, що питання керування інцидентами виникає не тільки в рамках забезпечення ІБ, але й при керуванні IT-сервісами в цілому. Сімейство міжнародних стандартів ISO/IEC 20000 в розділі Service Delivery and Support описує ряд вимог до організації процесу керування інцидентами в IT-інфраструктурі. Згідно з цими стандартами під *інцидентом* розуміється «*будь-яка подія, що не є елементом нормального функціонування служби і що при цьому надає або здатна зробити вплив на надання послуги служби шляхом її переривання або зниження якості*».

Процедура керування IT-інцидентами регулюється стандартом **ISO/IEC 20000** [4] (в Україні ДСТУ ISO/IEC 20000-2:2017 Інформаційні технології. Керування послугами. Частина 2. Настанова щодо застосування систем керування послугами (ISO/IEC 20000-2:2012, IDT) прийнятий 06.12.2017р.), який описує систему керування IT-сервісами та процедуру керування інцидентами, та розглядає IT-інциденти. Сама процедура керування інцидентами IT дуже близька до процедури керування інцидентами ІБ з тією різницею, що в останньому випадку більший акцент робиться на його розслідування, збір доказів, покарання винних.

З позицій ISO/IEC 20000 процес керування ІБ має два важливих значення:

– виконання вимог безпеки, закріплених в SLA (Service Level Agreement) та інших вимогах зовнішніх і внутрішніх угод, законодавчих актів і встановлених правил;
– забезпечення базового рівня ІБ, незалежного від зовнішніх вимог.

Вхідними даними для процесу служать SLA, що містять вимоги безпеки, за можливості, доповнені документами, що визначають політику організації в цій області, а також інші зовнішні вимоги. Процес також одержує важливу інформацію, що відноситься до проблем безпеки, з інших процесів, наприклад про інциденти, пов'язані з ІБ.

Вихідні дані включають інформацію про досягнуту реалізацію SLA разом із звітами про нештатні ситуації з погляду безпеки, а також інформацію про регулярні заходи щодо поліпшення СКІБ.

Вітчизняна нормативно-методологічна база з керування інцидентами ІБ.

Концепція [5] є інструментом реалізації державної політики в сфері телекомунікацій в Україні. У цій концепції (розділ «4. Розвиток телекомунікацій для потреб національної безпеки та оборони держави», підрозділ «Безпека телекомунікаційних мереж») є абзац, в якому визначено основні системоутворюючі засади та напрямки подальшого розвитку системи керування інцидентами:

«– створення державного координаційного центру з питань безпеки в інформаційно-телекомунікаційних мережах загального користування, сприяння створенню державних та недержавних центрів компетенції та реагування на інциденти в телекомунікаційних мережах».

Зміст документу НД ТЗІ 1.4-001-2000 [6] стосовно проблеми реагування та обробки інцидентів ІБ обмежується лише наступним:

«8.2 Функції під час експлуатації комплексної системи захисту інформації: ...– *розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій*».

Порядок [7] визначає основи організації та порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах (ІТС). В пункті 24 даного документу закріплено обов'язкове повідомлення про інциденти:

«*Власники АС та оператори МПД повинні повідомляти ДСТСЗІ СБ України про виявлені ними спроби та факти здійснення несанкціонованих дій щодо державних інформаційних ресурсів. Оператори МПД повинні надавати власнику АС відомості про виявлені ними спроби та факти здійснення несанкціонованих дій в мережах передачі даних щодо інформації, яка йому належить*».

Також про обов'язкове повідомлення про інциденти мова йдеться у статті 9 Закону України «Про захист інформації в інформаційно- телекомунікаційних системах» [8]:

«*Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації*».

Правила [9] визначають загальні вимоги та організаційні засади забезпечення захисту інформації, вимога щодо захисту якої встановлена законом. У пункті 11 цих правил сказано про обов'язкову реєстрацію інцидентів:

«*11. У системі здійснюється обов'язкова реєстрація: ...спроб несанкціонованих дій з інформацією; ...*

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, і службовою інформацією повинна супроводжуватися повідомленням про них адміністратору безпеки (відповідальній особі)».

В різних статтях Кримінального кодексу України в несистематизованому вигляді наводяться визначення і відповідальність за комп'ютерні злочини. Розвиток суспільних відносин у сфері інформаційної безпеки суттєво випереджає розвиток права у цих питаннях. Методів і засобів розслідування злочинів такого роду поки недостатньо, а законодавство ще не відповідає сьогоденним вимогам.

В рамках Адміністрації Держспецзв'язку України створений підрозділ (український аналог CSIRT), діяльність якого спрямована на вирішення завдань реагування та обробки інцидентів, що порушили безперебійне функціонування ІТМ органів державної влади.

Практичне завдання:

Здійснити порівняльний аналіз вимог чотирьох довільно обраних нормативно-правових документів до управління інцидентами ІБ. Відобразити за можливістю посилання на офіційні сайти державних органів в мережі Internet та на сайті Верховної Ради України. Обов'язково до кожного нормативно-правового документа має бути анотація.

Теоретичні питання:

1. Розтлумачте різницю між поняттями подія ІБ та інцидент ІБ.
2. Назвіть основні міжнародні та національні нормативні документи, якими визначаються процедури управління інцидентами ІБ.
3. Назвіть етапи управління інцидентами ІБ відповідно до ISO/IEC 27035.
4. Якими є цілі управління інцидентами інформаційної безпеки?
5. Опишіть особливості управління інцидентами ІБ відповідно до ITIL.
6. Сформулюйте основний принцип застосування міжнародних та національних стандартів, що описують управління інцидентами ІБ.
7. Для чого організації необхідні нормативні документи з управління інцидентами ІБ?

Лабораторна робота №2

Системи моніторингу та управління інформаційною безпекою

Мета роботи – ознайомитися з поняттям системи моніторингу, аналіз процесу впровадження системи моніторингу подій інформаційної безпеки та її функціонування.

Теоретичні відомості

З кожним днем зростає складність і кількість різних загроз інформаційної безпеки. Разом з цим збільшується і число систем, покликаних захистити бізнес від цих загроз. У 99% великих компаній функціонує міжмережевий екран, антивірусне рішення і система виявлення вторгнення – це сьогодні необхідний мінімум. Крім того, в мережі працюють бази даних, операційні системи та програмне забезпечення власної розробки. Всі ці підсистеми генерують реєстраційні журнали і різні події.

У підсумку адміністратори отримують сотні тисяч повідомлень від множии різноманітних підсистем кожен день. Функціонування кожної з підсистем окремо важливе для бізнесу в цілому, тому фахівці змушені аналізувати весь цей потік інформації. Виділити важливі повідомлення стає все складніше, і в результаті цінність окремих рішень для забезпечення безпеки прагне до нуля, а час відновлення інформаційної системи після збоїв катастрофічно зростає.

Максимально ефективно використовувати дані, одержані від сенсорів (серверів) виявлення атак та від міжмережевих екранів (про відхилені ними атаки) дозволяє використання системи моніторингу інформаційної безпеки. Система моніторингу ІБ дозволяє звести всі події та інциденти ІБ в єдиній консолі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи. Крім цього, система моніторингу ІБ виконує реєстрацію та зберігання всіх подій інформаційної безпеки, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та судочинстві.

Подієвий аналіз є одним із найбільш розповсюджених методологічних засобів вивчення динаміки ситуацій з інформаційною безпекою. Методика аналізу ґрунтується на спостереженні за розвитком та інтенсивністю подій (інцидентів з інформаційною безпекою) з метою визначення тенденцій.

Моніторинг – безперервне спостереження за станом оточуючого середовища з метою управління ним шляхом своєчасного інформування про можливості настання несприятливих, критичних або неприпустимих ситуацій у галузі ІБ. Моніторингові дослідження широко застосовуються для вивчення різноманітних об’єктів з метою прогнозу їх розвитку. Моніторингові

дослідження передбачають одержання статистичних або змістових показників, які характеризують об’єкт спостереження і які можна виміряти. Система спостережень будується на фіксації дискретних кількісних характеристик об’єкта спостереження, накопичуванні цих відомостей і на можливості шляхом інтелектуальної інтерпретації одержаних відомостей зробити висновки про якісний стан об’єкта. Моніторинг ґрунтується на спостереженні типових рис у поведінці об’єктів спостереження і на своєчасній фіксації на їх фоні різних відхилень від норми.

Сучасні кіберзлочинці не атакують безпосередньо IT-інфрастуктуру. Вони діють завуальовано, використовуючи вразливості захисних ресурсів. Такі інциденти залишаються поза увагою, через те, що без «контексту» не вказують на загрозу. Відстежити протиправні дії допомагає постійний моніторинг і аналіз всіх подій, що відбуваються в IT-інфраструктурі компанії. Таку здатність аналізувати та виявляти інциденти по окремим подіям мають SIEM-рішення (рис. 2.1).

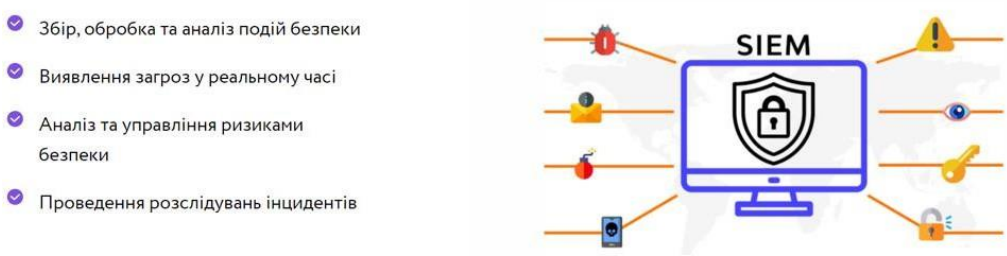

Рисунок 2.1 – Технологія SIEM захисту

Впровадження системи моніторингу подій інформаційної безпеки дозволить компанії досягти наступних переваг:

– забезпечити централізоване управління подіями і інцидентами ІБ;
– збільшити швидкість виявлення, розслідування та реагування на інциденти;
– управляти інцидентами ІБ;
– підвищити ефективність управління ризиками ІБ;
– підвищити рівень відповідності політикам і нормативним вимогам.

Також для ефективного захисту інформації, однією з головних складових є наявність операційного центру безпеки.

Операційний центр безпе́ки (Security Operations Center, SOC) – централізований підрозділ установи, який вирішує питання з інформаційної та кібербезпеки на організаційному та технічному рівні. Операційний центр безпеки (ОЦБ) – це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюється, оцінюється та захищається.

Первинна функція ОЦБ – аналіз на основі поточного моніторингу подій

інформаційної безпеки. Далі за пріоритетністю ідуть виявлення загроз, відповідь на інциденти безпеки та виправлення наслідків кожної ідентифікованої події.

ОЦБ об'єднує людей, процеси та технології для забезпечення обізнаності в поточній ситуації щодо інформаційної безпеки. В організації, частиною якої є ОЦБ, він розбирається з будь-якою загрозливою подією щодо інформаційної безпеки. Це включає належну ідентифікацію, аналіз, інформування, розслідування та подальше звітування. ОЦБ також веде моніторинг застосунків для виявлення можливої кібератаки чи вторгнення (тобто, події інформаційної безпеки), і визначає можливу шкоду для діяльності організації.

Одним із завдань ОЦБ є навчання та інформування користувачів, зокрема, прищеплення їм культури кібербезпеки, а також оперативне інформування про виникнення загроз та план дій на випадок кібератак. Без такої роботи з користувачами кібербезпека може виявитися неефективною.

Часто термін ОЦБ помилково прирівнюють до поняття SIEM, яке об'єднує керування інформаційною безпекою та подіями безпеки. SIEM представлений застосунками, приладами чи послугами, він також використовується для журналювання даних та генерації звітів задля сумісності з іншими даними організації. ОЦБ в свою чергу є комплексом програмно-технічних засобів, кваліфікованого персоналу та процесів їхньої взаємодії. ОЦБ також має такі завдання, як: адміністрування засобів гарантування інформаційної безпеки, постійний контроль за вразливостями в периметрі та в підконтрольних системах всередині мережі, контроль за привілейованими користувачами тощо.

Практичне завдання:

1. Ознайомитися з теоретичними відомостями.
2. Розробити короткий конспект-характеристику світових лідерів-постачальників SIEM систем.
3. Розробити короткий конспект-характеристику найбільш популярних SIEM-систем в Україні на теперішній час.
4. Зробити висновки.

Теоретичні питання:

1. Що таке системи моніторингу?
2. З яких джерел SIEM-системи використовують інформацію?
3. Функції SIEM-системи.
4. SIEM не протидіє зловмисним діям порушників, однак дозволяє отримати найбільш повне уявлення про виникаючі події безпеки. Чи згодні ви з цим твердженням? Поясніть чому.

Лабораторна робота №3

Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки

Мета роботи **–** ознайомитись зі сценарієм та описом життєвого циклу управління процесів згідно з моделлю PDCA.

Теоретичні відомості

Принципи інформаційної безпеки інтегровані в усі аспекти управління процесами та інформаційними технологіями сучасних організацій та підприємств. В цьому контексті йдеться про управління інформаційною безпекою (ІБ), класифікацію інформаційних активів, здійснення оцінки ризиків ІБ, забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків, моніторинг подій ІБ та управління інцидентами ІБ, забезпечення безперервності бізнес-діяльності підприємства, безпечне управління життєвим циклом інформаційних систем (ІС).

Метою забезпечення інформаційної безпеки організацій та підприємств є зниження ризиків щодо інформаційних ресурсів, що в свою чергу обумовлюється усуненням або мінімізацією збитку від можливих інцидентів інформаційної безпеки. Отже для забезпечення ІБ підприємствам доцільно враховувати вирішення завдань, пов’язаних з виявленням та обліком інцидентів ІБ, вчасним реагуванням на них, плануванням превентивних заходів захисту щодо забезпечення інформаційної безпеки.

Для управління інцидентами ІБ підприємству необхідно реалізувати можливість своєчасного виявлення інцидентів та адекватного реагування на них відповідними контрзаходами. У цьому відношенні з метою моніторингу захищеності інфраструктури, управління інцидентами ІБ, контролю відповідності вимогам в структурі сучасних підприємств представлені центри управління ІБ, що здійснюють пошук та усунення вразливостей, аналіз зовнішніх та внутрішніх джерел щодо актуальних кіберзагроз та розробку заходів щодо захисту, збору, аналізу та аудиту журналів подій в системі, а також виявлення, аналіз, реагування на інциденти та розробку заходів щодо покращення діючих процесів та заходів ІБ на основі отриманого досвіду.

Обробка інцидентів передбачає визначення їх пріоритетів, що дозволяє оцінювати ймовірність реалізації ризиків і тяжкості наслідків від них, та відповідно своєчасно реагувати і розслідувати інциденти з найвищими ризиками. Пріоритет визначається впливом (комерційним збитком або потенційним пошкодженням, зокрема, бази користувачів, безпеки, репутації, бренду) та терміновістю (швидкодією щодо усунення ознак інциденту, зокрема витік даних

або активне поширення шкідливого програмного забезпечення).

Зазвичай інциденти обробляються відповідно до присвоєного їм пріоритету. Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, що сприяє оперативному відновленню нормальної роботи служб і зведення до мінімуму негативного впливу інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні. Особливості УІІБ регламентуються міжнародними та національними нормативними документами, зокрема, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27035, ISO/ IEC 27042 та ISO/IEC 27043, NIST SP 800-16 тощо.

Для опису процедури УІІБ використовують класичну модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга – модель PDCA. Відповідно до стандартів модель PDCA виступає як основа функціонування всіх процесів системи управління інформаційною безпекою.

Цикл PDCA – плануй (Plan), роби (Do), перевіряй (Check), впливай (Act). Застосування цієї моделі в різноманітних областях діяльності (наприклад, управління якістю) дозволяє ефективно керувати цією діяльністю на системній основі.

Цикл «Плануйте-Робіть-Перевіряйте-Впливайте» вперше був розроблений у 20-х роках XX століття Уолтером Шухартом (Walter Shewhart) і пізніше популяризований У. Едвардсом Демінгом (W. Edwards Deming). З цієї причини на нього часто посилаються як на Цикл Демінга.

Концепція PDCA є у всіх сферах нашого професійного та особистого життя і використовується постійно, формально чи неформально, свідомо чи підсвідомо у всьому, що ми робимо. Кожна діяльність, неважливо, наскільки вона проста або складна, підпадає під цей цикл, що ніколи не припиняється (рис.3.1).

Рисунок 3.1 – Модель PDCA - цикл Едварда Демінга

Підтримка у робочому стані та постійне підвищення здатності процесів може бути досягнуто шляхом застосування концепції PDCA на всіх рівнях усередині організації. Ця концепція застосовується як до стратегічних процесів високого рівня, до планування системи управління якістю або аналізу з боку керівництва, так і до простих виробничих видів діяльності, що є частиною процесів створення продукції.

Примітка до Пункту 0.2 ISO 9001:2000 пояснює, що цикл PDCA застосовується до процесів наступним чином:

«*Плануй*: установлюй цілі та процеси, необхідні для видачі результатів, що відповідають вимогам замовника та політиці організації.

Виконуй: впроваджуй процеси.

Перевіряй: контролюй та вимірюй процеси і продукцію, виходячи з політики, цілей та вимог до продукції, а також звітуй про результати.

Дій: вживай заходи для постійного поліпшення показників функціонування процесу».

У багатьох компаніях не завжди можливо простежити за зміною кількості та характеру інцидентів інформаційної безпеки – відсутня процедура управління інцидентами. Часто відсутність інцидентів не вказує на те, що система управління безпекою працює правильно, а означає лише, що інциденти не фіксуються або не визначаються.

Управління інцидентами – одна з найважливіших процедур управління інформаційною безпекою. Насамперед, важливо правильно і своєчасно усунути наслідки інциденту, а також мати можливість проконтролювати, які дії були виконані для цього. Необхідно також розслідувати інцидент, що включає визначення причин його виникнення, винних осіб і конкретних дисциплінарних стягнень. Далі, як правило, слід виконати оцінку необхідності дій щодо усунення причин інциденту, якщо потрібно – реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту. Крім цього, важливо зберігати всі дані про інциденти інформаційної безпеки, оскільки статистика інцидентів інформаційної безпеки допомагає усвідомлювати їх кількість, характер, та зміну в часі. За допомогою інформації про статистику інцидентів можна визначити найбільш актуальні загрози для компанії і, відповідно, максимально точно планувати заходи щодо підвищення рівня захищеності інформаційної системи компанії.

Розглянемо практичні рекомендації з даного питання. При створенні системи управління інцидентами критично важливо, щоб всі співробітники компанії розуміли, що забезпечення інформаційної безпеки в цілому і управління інцидентами зокрема є основними бізнес-цілями компанії. Потім слід розробити необхідні нормативні документи з управління інцидентами. Як правило, такі документи повинні описувати:

1. Визначення інциденту інформаційної безпеки, перелік подій, що є інцидентами (що в компанії є інцидентом).

2. Порядок оповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід оповіщати про інцидент).

3. Порядок усунення наслідків і причин інциденту.

4. Порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів).

5. Винесення дисциплінарних стягнень.

6. Реалізація необхідних коригувальних і превентивних заходів.

Визначення переліку подій, що є інцидентами, - важливий етап розробки процедури управління інцидентами.

Слід розуміти, що всі події, які не увійдуть до зазначеного переліку, будуть розглядатися як штатні (навіть якщо вони несуть загрозу інформаційній безпеці). Зокрема, інцидентами інформаційної безпеки можуть бути:

– відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання;
– порушення конфіденційності та цілісності цінної інформації;
– недотримання вимог до інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації);
– незаконний моніторинг інформаційної системи;
– шкідливі програми;
– компрометація інформаційної системи (наприклад, розголошення пароля користувача).

Як приклад інцидентів можна привести такі події, як неавторизована зміна даних на сайті компанії, залишення комп'ютера незаблокованим без нагляду, пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти тощо. У загальному випадку інцидент інформаційної безпеки визначається як окрема, небажана або несподівана подія інформаційної безпеки (або сукупність таких подій), що може скомпрометувати бізнес-процеси компанії або загрожує її інформаційній безпеці.

Важливо відзначити, що процедура управління інцидентами тісно пов'язана з усіма іншими процедурами управління безпекою в компанії. Оскільки інцидентом, в першу чергу, є недозволена подія, вона повинна бути кимось заборонена, отже, необхідна наявність документів, що чітко описують всі дії, які можна виконувати в системі та які виконувати заборонено. Наприклад, в одній з компаній співробітник зберігав на мобільному комп'ютері конфіденційні відомості компанії без застосування засобів шифрування. Після роботи він забрав комп'ютер додому і забув його в машині, яку залишив під вікнами будинку, а вночі машину зламали, і комп'ютер був вкрадений. Зловмисники отримали доступ до конфіденційної інформації компанії і могли продати її конкурентам. Крім цього, на комп'ютері зберігалася цінна інформація, яка не була

зарезервована на іншому носії. Такий інцидент міг статися в результаті того, що в компанії не були розроблені процедури поводження з мобільними комп'ютерами та зберігання на них інформації.

Винос комп'ютера за межі офісу компанії, відсутність засобів шифрування і резервного копіювання інформації – можливі порушення, а отже, причини інцидентів. Однак поки документально не зафіксовано, що це порушення (тобто у відповідних документах не описано, що це заборонено), співробітника неможливо притягнути до відповідальності і запобігти повторному виконанню неправомірних дій.

Важливо, щоб були налагоджені такі процедури, як моніторинг подій, своєчасне видалення не використовуваних облікових записів, контроль і моніторинг дій користувачів, контроль над діями системних адміністраторів та ін. В одній з компаній був зафіксований наступний інцидент: при звільненні з роботи системний адміністратор вкрав розроблюваний компанією програмний продукт і передав його конкурентам, які випустили програму на ринок під своїм товарним знаком. Крім цього, він додав зміни в інформаційну систему, в результаті яких після його звільнення функціонування певних її компонентів було порушено. Залучити адміністратора до відповідальності в даному випадку виявилося неможливо, тому що, по-перше, не виконувалася реєстрація його дій, по-друге, адміністратор міг видалити всі докази своїх неправомірних дій і, по-третє, не була налагоджена процедура збору доказів про інцидент. Крім цього, в компанії просто не знали, як слід чинити в таких випадках (наприклад, можна було звернутися в спеціалізовану компанію з розслідування інцидентів або подати заяву до суду).

Практичне завдання:

1. Ознайомитися з теоретичними даними.
2. Самостійно розглянути принципи OECD.
3. Зробити таблицю порівняння та відповідності процесів OECD та PDCA.
4. Зробити висновки.

Теоретичні питання:

1. Як можна охарактеризувати цикл Шухарта–Демінга?
2. Мета забезпечення інформаційної безпеки організацій та підприємств.
3. Що таке інцидент інформаційної безпеки? Наведіть приклади.
4. Охарактеризуйте концепцію PDCA.

Лабораторна робота №4

Методи та моделі управління інцидентами інформаційної безпеки

Мета роботи – здійснити аналіз моделі управління інформаційною безпекою та аналіз моделей розслідування інцидентів кібербезпеки.

Теоретичні відомості

Згідно прийнятому в ITIL визначенню під «інцидентом» розуміється «будь-яка подія, що не є елементом нормального функціонування служби і при цьому надає або здатна зробити вплив на роботу служби шляхом її переривання або зниження якості».

Основні категорії інцидентів:

Додатки:

– служба недоступна;
– помилка в додатку, що не дає змогу клієнту нормально працювати;
– вичерпано дисковий простір.

Устаткування:

– збій системи;
– внутрішній сигнал тривоги;
– відмова принтера.

Заявки на обслуговування:

– надходження заявки на отримання додаткової інформації, поради, документації;
– забутий пароль.

Більшість груп IT-фахівців має відношення щодо усунення тих або інших інцидентів. Служба Service Desk відповідає за моніторинг процесу усунення всіх зареєстрованих інцидентів, оскільки є власником всіх таких інцидентів. Цей процес більшою мірою реактивний; для ефективної реакції на інциденти повинен бути визначений формальний метод роботи співробітників, що включає використання необхідного програмного забезпечення.

Використовувані для виявлення інцидентів процедури збору інформації можуть забезпечуватися як технічними, так і організаційними заходами; наприклад, відповідно до вимог політики безпеки, співробітник, що знайшов порушення, зобов'язаний повідомити про нього в підрозділ інформаційної безпеки. Потім інформація про виявлені інциденти фіксується в спеціальних журналах (в паперовому або електронному вигляді).

Результати аналізу, розслідувань і профілактичних заходів звичайно оформляються у вигляді довідок, звітів або аналітичних записок і зберігаються в підрозділі ІБ.

Одночасно зі зростанням ролі IT у компанії зростає потреба в забезпеченні відповідного рівня сервісу, забезпеченні максимальної доступності IT-послуг. Бізнес-користувач повинен мати можливість працювати в будь-який час і отримувати рішення своїх проблем, якщо вони виникли, якнайшвидше. Саме на це націлена реалізація процесів управління інцидентами та проблемами.

Структури, які можуть бути використані командами реагування на інциденти (CSIRT):

- Централізована групи реагування на інциденти. Одна команда реагування на інциденти обробляє інциденти в рамках всієї організації. Ця модель є ефективною для невеликих організацій і для організацій з мінімальним географічним розташуванням в плані обчислювальних ресурсів.
- Розподілене реагування на непередбачувані ситуації команди. Організація має кілька команд реагування на інциденти, кожен з яких відповідає за певний логічний чи фізичний сегмент організації. Ця модель є ефективною для великих організацій (наприклад, одна команда на відділ) і для організацій з основними обчислювальними ресурсами у віддалених місцях (наприклад , одна команда для віддаленого географічного регіону, одна команда для основного місця розташування). Проте, команди повинні бути частиною єдиної скоординованої структури, процес реагування на інциденти має узгоджуватися всією організацією та супроводжуватися обміном інформацією серед команд. Це особливо важливо тому, що кілька команд можуть бачити компоненти одного інциденту або можуть обробляти подібні інциденти.
- Координаційні групи. Команда реагування на інциденти консультує інші команди, що їй не підпорядковуються. Наприклад, departmentwide команда може допомогти командам окремих установ. Ця модель може розглядатися як CSIRT для CSIRTs. Оскільки в центрі уваги даного документа є центральні та розподілені CSIRTs, модель координаційної групи не розглядається докладно.

Найчастіше зустрічається структурна система підтримки – багаторівнева модель, в якій зростаючий рівень технічних можливостей застосовується для вирішення інциденту або проблеми.

Фактичні ролі та розподіл відповідальності, використовувані в багаторівневій реалізації системи підтримки, можуть різнитися залежно від персоналу, діяльності або політики конкретної організації. Проте, наступний опис багаторівневої системи підтримки типовий для багатьох організацій.

Перший рівень підтримки

Організація (підрозділ), що представляє перший рівень підтримки зазвичай відноситься до оперативних служб. Як правило це диспетчерська служба, Call Center, Help Desk, Service Desk.

Ролі:

– Перший рівень підтримки гарантує, що встановлено і підтримується одноманітно виконуваний, вимірюваний відповідним чином, ефективний

процес управління інцидентами.

– Отримання і керування всіма запитами щодо обслуговування споживачів. Перший рівень підтримки є єдиною точкою контакту для передачі запитів, і він діє як адвокат кінцевого користувача, який гарантує, що проблеми з обслуговуванням вирішуються своєчасно.
– Організація першого рівня підтримки робить першу спробу вирішити проблему з обслуговуванням, про яку повідомив кінцевий користувач.

Обов'язки:

– Точна реєстрація інцидентів. Перший рівень підтримки гарантує, що інформація про інцидент вноситься до журналу системи.
– Володіння кожним інцидентом. Як адвокат кінцевого користувача перший рівень підтримки забезпечує успішне вирішення кожного інциденту.
– Здібності та навички. Персонал першого рівня підтримки залучений головним чином в розстановку пріоритетів і керування проблемами. На цьому рівні підтримки проводяться лише незначні технічні вишукування.

Другий рівень підтримки

Цей рівень також зазвичай відноситься до оперативних служб.

Ролі:

– Дослідження інцидентів. Цей рівень підтримки вивчає, діагностує і вирішує більшість інцидентів, які не були вирішені на першому рівні. Ці інциденти мають тенденцію вказувати на нові проблеми.
– Запобіжне управління інфраструктурою. Використовує інструменти і процеси, щоб гарантувати, що проблеми виявляються і вирішуються до виникнення інцидентів.

Обов'язки:

– Рішення інцидентів, переданих з першого рівня. Якщо для першого рівня підтримки очікується, що він вирішує 80% інцидентів, то від другого рівня підтримки очікується, що він вирішує 75% інцидентів, переданих йому першим рівнем, тобто 15% від числа зареєстрованих інцидентів. Решта інцидентів передаються на третій рівень.
– Визначення причин проблем. Визначає причини проблем, які виникли і пропонує заходи щодо їх уникнення або усунення. Вони залучають і управляють іншими ресурсами відповідно до потреб визначення причин.
– Забезпечення реалізації виправлень і усунень проблем. Забезпечує ініціювання проектів в організаціях розробниках для реалізації планів усунення відомих помилок.
– Постійне вдосконалення процесу управління проблемами та ін.
– Здібності та навички (технічно компетентні з розумними навичками спілкування; знання мереж, серверів і додатків).

Третій рівень підтримки

Цей рівень підтримки зазвичай відноситься до групи розробки додатків і

мережевої інфраструктури.

Ролі

– Планування та проектування IT – інфраструктури;
– Останній рубіж в ескалації. Якщо інцидент або проблема виявляється вище можливостей групи підтримки другого рівня, то група підтримки третього рівня приймає відповідальність за пошук рішення.

Обов'язки

– Рішення інцидентів, переданих з другого рівня. Оскіьки більшість інцидентів викликається відомими помилками , то дуже небагато інцидентів (5%) проходить через другий рівень на третій. Третій рівень відповідає за вирішення всіх інцидентів, які до них надходять.
– Участь у діяльності з управління проблемами. Задіяний в пошуку причин, способів обходу та усунення помилок.
– Реалізація заходів щодо усунення помилок в інфраструктурі. Значна роль полягає у плануванні, конструюванні та реалізації проектів щодо усунення недоліків інфраструктури.
– Здібності та навички (експерти, які планують і проектують IT-інфраструктуру).

Практичне завдання:

1. Ознайомитися з теоретичними даними.
2. Розробити рекомендації щодо організації успішного управління інцидентами.
3. Зробити висновки.

Теоретичні питання:

1. Охарактеризуйте структурну систему підтримки.
2. Основні категорії інцидентів.
3. Здійсніть аналіз кожного рівня підтримки.

Лабораторна робота № 5

Діяльність у рамках процесу управління IT-інцидентами

Мета роботи – ознайомлення з основними етапами управління IT- інцидентами інформаційної безпеки.

Теоретичні відомості

Управління IT-інцидентами – це один із основних процесів у роботі служби підтримки. IT-інцидент – це порушення в роботі IT-служб організації, що впливає як на окремого користувача, так і на організацію в цілому. Якщо говорити коротко, інцидент – це будь-яка ситуація, яка перериває безперебійну роботу бізнесу.

Управління інцидентами – це процес управління порушеннями у роботі IT-служб та відновлення їх працездатності протягом терміну, зазначеного в угоді про рівень обслуговування (SLA).

Область управління інцидентами починається з моменту повідомлення кінцевим користувачем про проблему та закінчується усуненням проблеми спеціалістом служби підтримки.

Організовуючи управління інцидентами належним чином, можна оптимізувати збір інформації про інциденти та впорядкувати її, позбавившись плутанини в листуванні електронною поштою. Спеціалісти служби підтримки можуть опублікувати відповідні форми на порталі самообслуговування для користувачів, щоб забезпечити своєчасне збирання всієї необхідної інформації при створенні заявки.

Наступний етап управління інцидентами передбачає класифікацію інциденту та присвоєння йому пріоритету. Це не тільки допомагає сортувати заявки, що надходять, але й гарантує переадресацію заявки тим фахівцям, які мають всі необхідні знання і навички для усунення проблеми. Завдяки класифікації до інцидентів застосовуються найбільш відповідні SLA, а кінцеві користувачі можуть дізнатися пріоритет своїх звернень. Після того, як інциденту присвоєно клас та пріоритет, технічні фахівці можуть виконати діагностику та надати кінцевому користувачеві відповідне рішення.

За наявності відповідних процесів автоматизації управління інцидентами дозволяє спеціалістам служби підтримки відстежувати дотримання SLA. Також можна настроїти повідомлення технічних фахівців про порушення SLA. Технічні фахівці також можуть ескалувати порушення SLA або налаштувавши автоматичну ескалацію, коли це застосовно до інциденту. Після діагностики проблеми технічний фахівець пропонує кінцевому користувачеві рішення, яке може перевірити останній. Цей багатоетапний процес забезпечує оперативне

усунення ІТ-проблем, які впливають на безперебійну роботу бізнесу.

Завданнями процесу управління інцидентами є:

– Забезпечення використання стандартних методів та процедур ефективного та оперативного реагування, аналізу, документування, поточного управління та звітності під час вирішення інцидентів.
– Підвищення прозорості та комунікацій при вирішенні інцидентів між бізнесом та ІТ.
– Поліпшення сприйняття бізнесом ІТ через професійний підхід до вирішення інцидентів.
– Поєднання пріоритетів у вирішенні інцидентів із пріоритетами бізнесу.
– Підтримка задоволеності користувачів якістю ІТ-послуг.

Інциденти можуть виникнути у будь-якій частині інфраструктури. Часто про них повідомляють користувачі, але й можливе їх виявлення ІТ-співробітниками на основі інформації від систем моніторингу.

Найчастіше інциденти реєструються Service Desk, куди надходять повідомлення про них. Реєстрація всіх інцидентів повинна провадитися негайно після надходження повідомлення з наступних причин:

– важко зробити точну реєстрацію інформації про інцидент, якщо це не зроблено відразу;
– моніторинг ходу робіт з розв’язання інциденту можливий лише якщо інцидент зареєстрований;
– зареєстровані інциденти сприяють діагностиці нових інцидентів;
– управління проблемами може використовувати зареєстровані інциденти під час пошуку кореневих причин;
– легше визначити рівень впливу, якщо всі повідомлення (дзвінки) зареєстровані;
– без реєстрації інцидентів неможливо контролювати виконання домовленостей (SLA);
– негайна реєстрація інцидентів запобігає ситуації, коли або кілька людей працюють над одним і тим самим інцидентом, або ніхто нічого не робить для вирішення інциденту.

Вся значуща інформація про інцидент має бути зафіксована і доступна групам підтримки.

При початковій реєстрації інциденту має бути проведена його категоризація.

Категорія – названа група об'єктів, що мають щось спільне. Категорії використовують для об'єднання схожих об'єктів. Наприклад, типи витрат використовуються для угруповання однотипних витрат, категорії інцидентів – однотипних інцидентів, типи КО – однотипних конфігураційних одиниць.

Правильна категоризація інцидентів допомагає спрямувати їх одразу в потрібну групу, проводити аналіз інцидентів у різних розрізах, а також формує

основу для пошуку причин виникнення інцидентів та їх усунення у рамках процесу управління проблемами.

Кожному інциденту надається певний пріоритет – категорія, що використовується для визначення відносної важливості інциденту.

Пріоритет ґрунтується на впливі і терміновості та використовується для визначення необхідного часу обробки.

Терміновість (urgency) – міра того, наскільки швидко з моменту появи інцидент, набуде істотного впливу на бізнес.

Ступінь впливу (impact) – міра впливу інциденту на бізнес-процес.

Таким чином, фактично, пріоритет – це номер, який визначається терміновістю (наскільки швидко це має бути виправлено) і ступенем впливу (який збиток буде завдано, якщо не виправити швидко). Пріоритет = Терміновість × Ступінь впливу. З пріоритету визначається черговість усунення інцидентів.

Пріоритет встановлюється з урахуванням таких факторів: терміновість, вплив на бізнес, ризик для життя чи здоров'я (risk to life or limb), число порушених послуг, фінансові втрати, вплив на репутацію бізнесу, вплив на відповідність законам та іншим нормам тощо.

З урахуванням встановленого пріоритету та існуючих угод (SLA) користувач інформується про максимальний розрахунковий час вирішення інциденту (крайній термін). Ці терміни також фіксуються. Інциденту надається унікальний номер і користувач інформується про номер інциденту для його точної ідентифікації при наступних зверненнях.

Безпосередньо при зверненні користувача фахівцями Service Desk має бути проведена попередня діагностика інциденту для отримання необхідної інформації з метою встановлення причини інциденту, якщо це можливо, а також для коректної категоризації та передачі на наступну лінію підтримки. Якщо рішення інциденту перебуває у компетенції співробітника Service Desk, він може бути вирішений відразу. Служба Service Desk направляє інциденти, які не мають готового рішення або виходять за межі компетенції працівника, який працює з ним, групі підтримки наступного рівня з більшим досвідом і знаннями. Ця група досліджує та розв’язує інцидент або спрямовує його групі підтримки чергового рівня.

У процесі розв’язання інциденту різні фахівці можуть оновлювати реєстраційний запис про нього, змінюючи поточний статус, інформацію про виконані дії, переглядаючи класифікацію та оновлюючи час та код працівника, який з ним працював.

Найчастіше відповідальною за моніторинг ходу рішення є Служба Service Desk, як «власник» всіх інцидентів. Ця служба також повинна інформувати користувача про стан інциденту. Зворотний зв'язок з користувачем може бути доречним після зміни статусу, наприклад, спрямування інциденту на наступну

лінію підтримки, зміну розрахункового часу рішення, ескалації тощо.

Ескалація – діяльність, спрямована на отримання додаткових ресурсів, коли це необхідно задля досягнення цільових показників рівня послуги чи задоволення очікувань замовника. Ескалація може бути потрібна в рамках будь-якого процесу управління IT-послугами, але найчастіше асоціюється з управлінням інцидентами, управлінням проблемами та управлінням скаргами замовника. Існує два типи ескалації: функціональна та ієрархічна ескалація.

Після успішного завершення аналізу та розв’язання інциденту співробітник фіксує інформацію про застосоване рішення. Якщо на певний момент часу неможливий повний розв’язок інциденту, його вплив, якщо можливо, має бути знижений застосуванням обхідного рішення. У найгіршому випадку, якщо не виявлено жодного рішення, інцидент залишається відкритим.

Після реалізації рішення, що задовольняє користувача, група підтримки спрямовує інцидент у Service Desk. Service Desk зв'язується зі співробітником, який повідомив про інцидент, з метою оповіщення про успішне вирішення питання. Якщо він це підтверджує, інцидент може бути закритий; інакше процес відновлюється на відповідному рівні. При закритті інциденту необхідно оновити дані про остаточну категорію, пріоритет, послуги, що зазнали впливу інциденту, і конфігураційні одиниці, що викликали збій.

Практичне завдання:

1. Ознайомитися з теоретичними відомостями.
2. Визначте та опишіть основні етапи процесу управління інцидентами.
3. Зробити висновки.

Теоретичні питання:

1. Що відбувається, коли в організації немає управління IT-інцидентами?
2. Хто використовує керування IT-інцидентами?
3. Що таке процес управління інцидентами?
4. На якому етапі вживаються заходи для усунення інциденту та повернення системи до попереднього робочого стану?

Лабораторна робота №6

Автоматизація процесів управління інцидентами інформаційної безпеки

Мета роботи – здійснення порівняльну характеристику програмних продуктів автоматизації процесів управління інцидентами інформаційної безпеки.

Теоретичні відомості

Засоби управління інцидентами NetForensics

При автоматизації процесів управління інцидентами, в першу чергу, необхідно надавати увагу автоматизованій обробці подій кібербезпеки – основі практично будь-якого інциденту. Події від різних програмних та технічних засобів захисту є найважливішим постачальником інформації щодо процесів, що відбуваються в системі управління кібербезпекою, порушеннях, ризиках. На підставі подій проводяться коригуючі дії, оцінка поточної захищеності системи, ефективності функціонування СУІБ. Тільки володіючи повним та достовірним набором подій, можна провести належне розслідування інцидентів, отримати уявлення щодо динаміки розвитку СУІБ. Можна сказати, що події – основний канал зворотного зв'язку для управлінських дій в рамках СУІБ.

Організація процесу обробки подій без використання засобів автоматизації представляє собою складну та трудомістку задачу. Необхідно збирати і консолідувати велику кількість даних в різних форматах, вести центральний архів. Для ручної обробки подій необхідна велика кількість висококваліфікованих фахівців-аналітиків.

Для підтримки процесу обробки подій на рівні, відповідному сучасним вимогам, можливим є застосування різних автоматизованих систем обробки подій (СОП).

Системи обробки подій повинні забезпечувати наступний функціонал:

- дозволяти збирати події з усіх програмних та технічних засобів забезпечення захищеності, що використовуються в рамках СУІБ;
- виконувати нормалізацію подій, приводячи їх до єдиного формату;
- здійснювати зберігання подій шляхом, що дозволяє зберігати необхідні об'єми даних;
- надавати інструментарій для пошуку в сховищі даних;
- надавати механізми формування різного роду звітів;
- система обробки подій повинна бути розширюваною та масштабованою;
- опціонально здійснювати кореляцію зібраних подій.

Процес обробки подій автоматизованими системами включає наступні основні кроки: нормалізація (приведення до єдиного формату) даних, агрегація

(накопичення), кореляція і візуалізація. На перших двох стадіях інформація про події безпеки збирається практично зі всіх використовуваних в рамках СУІБ засобів захисту: міжмережевих екранів, систем виявлення атак, антивірусних систем, операційних систем і додатків різних виробників, засобів контролю фізичного доступу, і перетворюється в єдиний, зручний для розуміння формат. Зібрані дані піддаються кореляції і виводяться на консоль оператора системи.

Розвинуті засоби пошуку дозволяють проводити оперативне та всебічне розслідування інцидентів, забезпечувати підтвердження наявності і функціонування засобів захисту в рамках СУІБ при проведенні різних аудитів.

Характеристики netForensics

Зараз на ринку присутні автоматизовані системи, що реалізують необхідний функціонал. Один з кращий серед них - програмний продукт для обробки подій – netForensics (nFX) Open Security Platform (рис. 6.1).

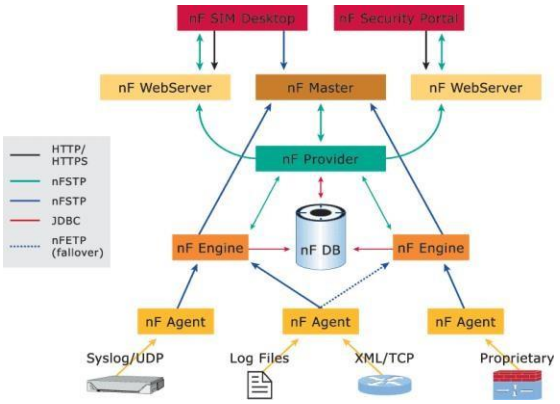

Рисунок 6.1 – СУІБ netForensics

Система управління інформаційною безпекою netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення кібербезпеки і реалізує безперервний збір, обробку і відображення подій безпеки. Система працює під управлінням ОС Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle. Описувана СУІБ має широкі можливості роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій. Система netForensics реалізована на базі технології Java за модульним принципом.

Основні модулі системи:

– сервер додатків – реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами;
– база даних – забезпечує зберігання інформації, що надходить в систему;
– модуль кореляції – здійснює кореляцію зібраних даних;
– модуль автоматизації управління інцидентами – здійснює автоматизацію процесів управління інцидентами;

– агенти – збирають інформацію безпосередньо з пристроїв.

До складу системи також входять засоби щодо написання агентів збору даних з нестандартних засобів захисту, засоби визначення користувацьких правил кореляції і створення звітів.

Встановлення та деінсталяція nFX Log One

Перш, ніж встановлювати дане програмне забезпечення необхідно переконатись в тому, що всі вимоги операційної системи до технічних засобів виконуються.

MS SQL Server з додатковим функціоналом Management Studio, а також Reporting Services, який необхідний для формування звітів. Дуже важливо в процесі інсталяції SQL серверу вибрати тип аутентифікації SQL authentication (Mixed mode) та використовувати пароль для запису «sa», який відповідає вимогам безпеки (більше 8 символів тощо).

Для установки даного ПЗ необхідні права локального адміністратора.

Протягом процесу установки, буде запропоновано надати наступну інформацію:

– Ім'я користувача, назва компанії та серійний номер (наданий netForensics).
– Ваш вибір SQL серверу, щоб обслуговувати базу даних LogCaster.
– Місце призначення і розташування для системних файлів LogCaster.
– Ім'я SQL серверу.
– SQL сервер адміністраторське оточення з паролем.
– Ім'я бази даних LogCaster.

Консоль управління nFX Log One

Консоль управління nFX Log One є важливою частиною програмного забезпечення nFX Log One, оскільки це те середовище, де розмішується, управляється та контролюється вся функціональність nFX Log One. Консоль управління nFX Log One забезпечує єдиним, консолідованим інтерфейсом для реєстрації інформації зібраної агентами nFX Log One.

При реєстрації всередині консолі управління nFX Log One відобразиться наступне вікно (рис. 6.2):

Рисунок 6.2 – Вікно консолі управління логіном

Поля, розміщені на даному екрані описуються у таблиці 6.1.

Таблиця 6.1 – Опис екрану nFX Log One Login

Ім’я поля	Опис
User ID (Ім’я користувача)	Визначає які права ви маєте в межах консолі управління nFX Log One.
Password (Пароль)	Пароль Windows для ім’я користувача, який був введений.
Domain (Домен)	Домен Windows, де знаходиться ваше ім’я користувача. Залиште порожнім це поле, якщо ваш комп’ютер є частиною робочої групи.
Dispatcher (Диспетчер)	Ім’я домену Windows для сервера комп’ютера nFX Log One.
Port (Порт)	Порт, який використовується сервером nFX Log One для управління запитами консолі nFX Log One.
VPN Key (Ключ VPN)	Віртуальна особиста мережа залишає це поле для використання внутрішнього 128-бітного ключа кодування nFX Log One.
Update Rate (Норма модифікації)	Визначає як часто оновлюється інформація в консолі управління nFX Log One.

Опція *конфігурації користувача*, яка сформована для адміністрування, дозволяє створювати та змінювати користувачів. Створений користувач отримує доступ до інформування про певні події, що відбувається через встановлення специфіки зв'язку користувача і планування часу.

Опція *розкладу сповіщення* дозволяє визначити годину дня та день тижня, який користувач вважатиме відпрацьованим, таким чином сповіщення через електронну пошту або месенджер повинно бути відправлене. Виділені години – це години, протягом яких користувач одержить сповіщення.

Крім того, є можливість групувати комп'ютери Агентів та Користувачів (Users) в ділових групах для організаційних цілей та встановлення Груп сповіщення. Також можна застосувати Груповий рівень привілей щодо ділових груп або створювати специфічні привілеї ділових груп для специфічних користувачів.

Спостерігач подій (Event Watcher)

Правила спостерігача подій перераховуються в пріоритетному порядку, зі всіма груповими правилами контейнера, що приймає на себе вищий пріоритет, ніж ділові групи, включаючи підприємницьку групу. Коли нова подія генерується на комп'ютері агента, це порівнюється з кожним правилом списку всіх груп відразу через правила, що перераховані в інших ділових групах. Коли подія знаходить відповідне правило, nFX Log One Agent виконує будь-яку дію,

конкретизовану в межах цього правила.

Спостерігач подій дозволяє об'єднати події, зібрані зі всіх агентних комп'ютерів до одного спільного екрану (рис. 6.3).

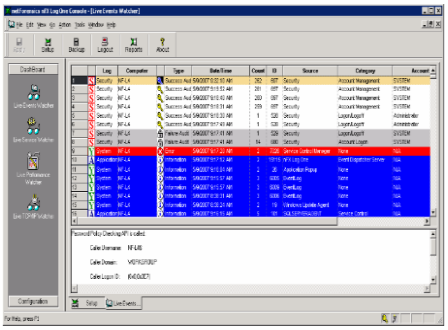

Рисунок 6.3 – Вікно спостерігача подій

Інформація надана у верхній частині Live Events Watcher екрану, показується в колонках.

Правила спостерігача подій

nFX Log One працює з широким набором вбудованих стандартних правил, допомагаючи у відстеженні внутрішньої безпеки і перевірки. Спостерігач подій забезпечений п'ятьма видами правил фільтра (Event Watcher Filter), включаючи:

– Правило подій.
– Правило спостерігача за подіями.
– Правило, створене з включеної бази даних стандартної події.
– Правило, створене зі звіту подій.
– Правило, імпортоване із шаблону додатку.

Вікно створення правила події має наступний вигляд (рис. 6.4):

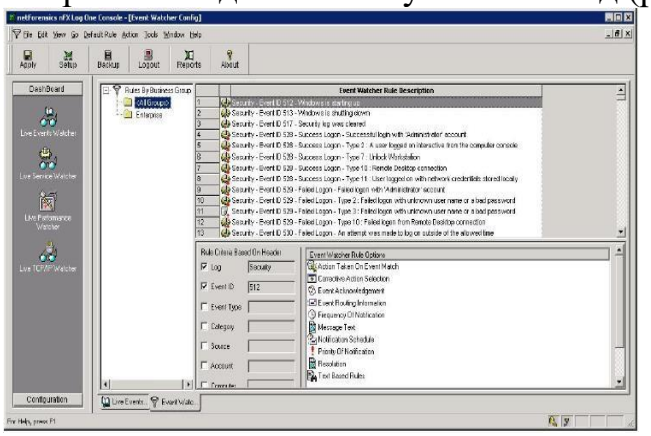

Рисунок 6.4 – Вікно Event Watcher Config

Дане вікно ділиться на чотири розділи.

Розділ опису правил спостерігача подій (Event Watcher Rule Description) вміщує правила, вже розміщені для бізнес групи, які виділяються в розділі правил бізнес групи.

Розділ правил бізнес групи вміщує бізнес групи, створені в процесі

інсталяції ПЗ. Цей розділ також вміщує за замовчанням групу, яка зветься <Всі групи (All Groups)>, яка використовується в тих випадках, коли ви хочете звернутися до правила спостерігача подій всіх бізнес груп.

Критерій правила, що базується на розділі Header, вміщує варіанти, які повинні бути представлені в події для дій, розташованих в розділі варіантів правила спостерігача подій (Event Watcher Rule Options).

Розділ варіантів правила спостерігача подій (Event Watcher Rule Options), це той розділ, в якому визначається які дії буде виконувати ПЗ, коли варіанти в розділі Критерій правила, що базується на розділі Header, є зустрічними з подією.

З вікна *опису правила спостерігача подій* (Event Watcher Rule Description) можна виконати окремі ключові функції, включаючи:

– Перейменування правила спостерігача подій.
– Переміщення або копіювання правила спостерігача подій в бізнес групу.
– Переміщення правила спостерігача подій вгору або вниз в межах списку правила.
– Переміщення правила спостерігача подій на верх списку правила спостерігача подій.

Критерій правила, що базується на Header Subscreen визначає, чи подія Windows відповідає одному з правил спостерігача подій nFX Log One.

Також можна додавати інші критерії, використовуючи вкладку правила, які засновані на тексті (Text Based Rules):

Вікно варіантів правила спостерігача подій містить 10 конфігураційних варіантів для кожного правила:

– Дія, покладена на узгодженість події.
– Відбір коригуючої дії.
– Підтвердження події.
– Подія, що відсилає інформацію.
– Частота сповіщення.
– Текст повідомлення.
– Розклад сповіщення.
– Пріоритет сповіщення.
– Резолюція.
– Правила, що базуються на тексті.

За замовчанням, всі нові розміщені правила спостерігача подій автоматично передаються узгоджуючій події на сервер.

Вікно опису правила спостерігача має такий вигляд (рис.6.5):

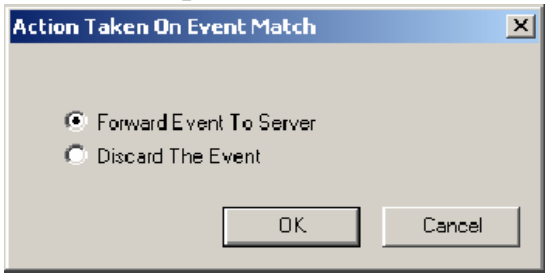

Рисунок 6.5 – Вікно дії, покладеної на узгодженість події

Виберіть наступні варіанти: або відіслати подію на сервер (Forward Event To Server) або відхилити подію (Discard The Event).

Варіант відбору корегуючої дії дозволяє налаштувати nFX Log One, щоб виконати звичайний сценарій або командний файл, якщо специфічна подія прописана на реєстрацію події Windows.

Крім того, правила подій можуть бути налаштовані для надання резолюції і відправлення підтверджуючої електронної пошти адміністратору або допомоги групам.

Панель підтвердження необхідної події для специфічного правила має вигляд (рис. 6.6):

Рисунок 6.6 – Вікно підтвердження події

Вікно варіанту події, що відсилає інформацію зображено на рисунку 6.7.

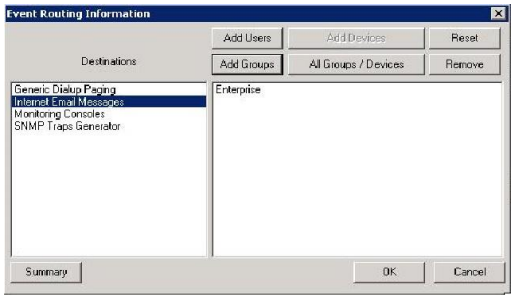

Рисунок 6.7 – Вікно події, що відсилає інформацію

Варіант частоти сповіщення визначає як часто сповіщення повинне бути згенероване. Іншими словами, це дозволяє вам повідомити nFX Log One коли і як часто ви хотіли б бути сповіщеними повторюваними простими типами подій (рис. 6.8).

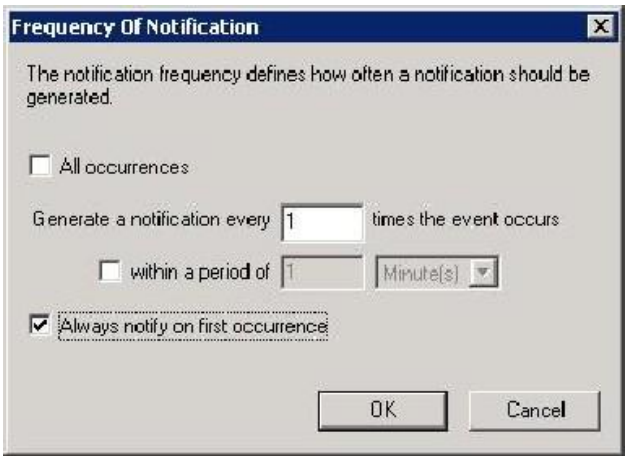

Рисунок 6.8 – Вікно частоти сповіщення

Варіант тексту повідомлення – швидкий та зручний шлях, щоб побачити текст повідомлення події, для якої було створене специфічне правило. Варіант текстового повідомлення може також бути використаний для копіювання або вставки інформації перейменування правил спостерігача подій.

Варіант розкладу сповіщення дозволяє визначити як годину дня, так і день тижня, в якому специфічне правило буде активним (рис. 6.9).

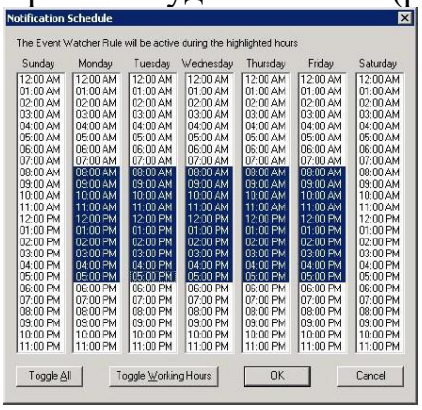

Рисунок 6.9 – Вікно розкладу сповіщення

Варіант пріоритету сповіщення дозволяє класифікувати важливість сповіщення, заснованого на масштабах від 0 до 100, з 0 – існування найважливіших та 100 – існування найменш важливих сповіщень (рис.6.10).

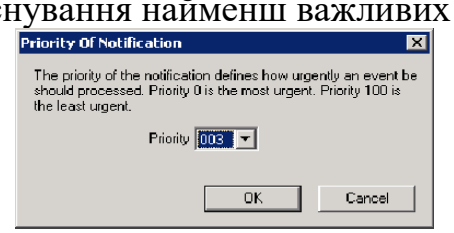

Рисунок 6.10 – Вікно пріоритету сповіщення

За допомогою варіанту *тексту резолюції*, можна додати звичайний текст повідомлення або інструкції до події, щоб допомогти користувачам дієво вирішити завдання (рис. 6.11).

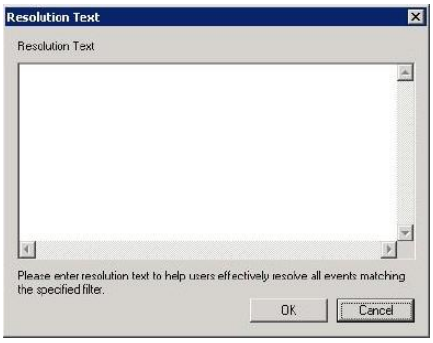

Рисунок 6.11 – Вікно тексту резолюції

Варіант правил, що базуються на тексті дозволяє додавати подальші критерії щодо розміщеного правила. За допомогою додавання заснованих на тексті правил або ключових слів, nFX Log One не враховуватиме схожість правила за винятком або текстового рядка або всіх ключових слів представлених в текстовому повідомленні події (рис. 6.12).

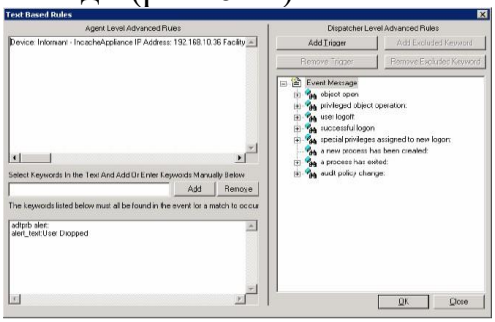

Рисунок 6.12 – Вікно правил, заснованих на тексті

Спостерігач текстового файлу – могутній інструментальний засіб, який дозволяє перетворити будь-які записи текстового файлу на подію Windows для більш легкого контролю. Більшість додатків генерує реєстрації для своєї власної діяльності; проте, ці реєстрації не можуть бути представлені за межами окремих додатків. Це може обмежити придатність реєстрації додатку, тому що системні адміністратори не можуть активно спостерігати за реєстраціями в реальному часі або з віддаленого іншого комп'ютера.

За допомогою спостерігача текстового файлу nFX Log One можна генерувати Windows події, що базуються на тексті написані до реєстрації додатку або текстового файлу, а потім використовувати маршрут обробки nFX Log One для того щоб бути сповіщеним за допомогою месенджера, електронної пошти тощо.

Можна створити звичайні правила спостерігача текстового файлу або створити, або імпортувати шаблон, який потім може звертатися до одного або більше файлів з тим же текстовим форматом.

Інструментальні засоби супроводу програми nFX Log One:

– Огляд інструментального засобу супроводу програми.

– Інструментальний засіб блокування рівней контролю.
– Інструментальний засіб перезавантаження.
– Інструментальний засіб виконання.
– Менеджер розкладів.
– Сервіс менеджер.
– Інструментальний засіб контролю журналу подій.
– Інструментальний засіб пильного технічного обслуговування.
– Інструментальний засіб конфігурації бази даних.
– Інструментальний засіб управління квотою бази даних.
– Функції перенесення (бекап) та відновлення.

nFX Log One пропонує повний набір інструментальних засобів управління, які працюють в поєднанні з базовою функціональністю nFX Log One, для полегшення задач системи та технічного обслуговування мережі. Розглянемо ці інструментальні засоби.

Інструментальний засіб блокування рівней контролю – дозволяє nFX Log One блокувати певні визначені користувачем рівні контролю, підіймати тривогу та коректувати дії протягом визначеного періоду часу таким чином, що, наприклад, підтримка системи може бути виконана без помилкового сповіщення.

Інструментальний засіб перезавантаження – автоматизує перезавантаження системи та дозволяє встановити розклад перезавантаження окремого або групи комп'ютерів.

Інструментальний засіб виконання – автоматизує запускання та виконання програм на комп'ютері або групі комп'ютерів, і дозволяє встановити розклад виконання на регулярній основі.

Менеджер розкладів – надає легкий доступ до всіх запланованих за розкладом заблокованих рівней контролю, перезавантажень, виконання задач та звітів.

Сервіс менеджер – дозволяє контролювати будь-який віддалений або локальний сервіс в будь-якій системі, де розташований nFX Log One Agent.

Інструментальний засіб контролю журналу подій – дозволяє користувачеві визначити конфігурацію властивостей всіх журналів подій Windows на всіх системах працюючих з nFX Log One Agent.

Інструментальний засіб пильного технічного обслуговування тривог – дозволяє зупинити незакінчені тривоги від початку існування до їх призначеного отримувача. Цей інструментальний засіб є надзвичайно корисним для контролю помилково піднятої тривоги журналу nFX Log One, взятого користувачем за основу.

Інструментальний засіб конфігурації бази даних – дозволяє змінити базу даних nFX Log One, використовуючи для зберігання всі оперативні дані та інформацію про конфігурацію.

Інструментальний засіб управління квотою бази даних – дозволяє

визначити як довго дані зберігаються на вашому жорсткому диску.

Інструментальний засіб резервного копіювання та відновлення– дозволить перенести всі конфігураційні файли nFX Log One до директорії nFX Log One.

Використання звітів в netForensics Reporting:

– Виконання звіту.
– Конфігурація звіту.
– Історія звіту.
– Підписи звіту.
– Доступ звіту та призначення ролі.

Операції, які можуть бути виконані над звітами та папками:

– Збереження звіту (Saving Report).
– Переміщення звітів (Moving Reports).
– Видалення звітів (Deleting Reports).
– Експорт звітів (Exporting Reports).
– Текстовий пошук повідомлення (Message Text Searching).
– Зміна логотипу звіту.
– Зміна налаштувань джерела даних DSN.

Практичне завдання:

1. Ознайомитися з теоретичними відомостями.
2. Використовуючи інформаційні ресурси мережі Internet, здійснити порівняльну характеристику двох програмних продуктів автоматизації процесу управління інцидентами інформаційної безпеки.
3. Зробити висновки.

Теоретичні питання:

1. Назвіть основні властивості параметрів користувача nFX LogOne.
2. За яким принципом будуються правила спостерігача подій?
3. Назвіть інструментальні засоби супроводу програми nFX Log One.
4. Опишіть використання звітів в netForensics Reporting.

Лабораторна робота № 7

Моніторинг та реєстрація інцидентів інформаційної безпеки

Мета роботи – здійснення оперативного моніторингу стану інформаційної безпеки досліджуваного об’єкта; розвиток практичних вмінь та навичок виявлення, реєстрації та аналізу інцидентів інформаційної безпеки.

Теоретичні відомості

Інцидент інформаційної безпеки - подія, що є наслідком одного або декількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації операції і створення загрози ІБ.

В свою чергу, подія інформаційної безпеки - ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути істотною для безпеки.

В загальному випадку, ознаки інциденту поділяються на дві основні категорії, повідомлення про те, що інцидент відбувається в даний момент і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому. Перерахуємо деякі ознаки здійснюваної події: крах web-інтерфейсу; працівники повідомляють про достатньо низьку швидкість при спробі виходу в мережу «Інтернет»; посадова особа, на яку відповідно до розподілу обов’язків покладені обов’язки системного адміністратора фіксує наявність файлів з підозрілими назвами; працівники повідомляють про наявність у своїх поштових скриньках багатьох повторюваних повідомлень; хост (вузол) вносить запис до журналу аудиту про зміну конфігурації; додаток фіксує в журнальному файлі множинні невдалі спроби авторизації; посадова особа, на яку відповідно до розподілу обов’язків покладені обов’язки адміністратора мережі фіксує різке збільшення мережевого трафіку тощо.

Прикладами подій, які можуть стати джерелами інформаційної безпеки можуть бути: журнальні файли сервера, які фіксують сканування портів; оголошення про появу нового виду експлойту (комп'ютерної програми, фрагменту програмного коду або послідовності команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему); відкрита заява комп'ютерних злочинців про наміри організації та інше.

Виявлення і реєстрація інциденту

Інцидент інформаційної безпеки може помітити працівник або посадова особа відповідальна за функціонування системи управління інформаційною безпекою. Для працівників має розроблятися інструкція, яка буде містити опис, в

якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попередити про те, що виконувати які-небудь дії самостійно заборонено). Такий звіт повинен містити докладний опис інциденту, перелік співробітників, залучених до інциденту, прізвище співробітника, що зафіксував інцидент та дату виникнення і реєстрації інциденту. Також повинні бути вказані дії для фахівця, до обов'язків якого входить реєстрація інциденту. Співробітник, що виявив інцидент, зв'язується із співробітником, відповідальним за реєстрацію інциденту для виконання подальших дій. Також співробітники можуть звернутися напряму до фахівця, який може усунути наслідки й причини інциденту (наприклад, до посадової особи відповідальної за функціонування системи управління інформаційною безпекою, або до посадової особи на яку відповідно до розподілу обов’язків покладені обов’язки системного адміністратора).

Ролі та відповідальність

Обов’язки щодо своєчасного реагування та розгляду інцидентів інформаційної безпеки покладаються на групу реагування на інциденти інформаційної безпеки (далі - ГРІІБ).

Основні цілі ГРІІБ:

– забезпечення організації кваліфікованим персоналом для обліку, реагування та аналізу інцидентів;
– забезпечення необхідної координації і управління процесом реагування на інциденти;
– забезпечення належного рівня інформування керівництва і зацікавлених осіб;
– забезпечення максимального зниження наслідків інцидентів як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи рекомендується включити:

– посадову особу відповідальну за функціонування системи управління інформаційною безпекою (забезпечення координаційної, адміністративної, експертної і технологічної діяльності);
– працівника, на якого покладено обов’язки служби інформаційних технологій;
– працівника відділу з питань служби в органах місцевого самоврядування і кадрової роботи (забезпечення адміністративної і процедурної діяльності);
– працівника юридичного відділу (забезпечення експертної і нормативно-правої діяльності);
– працівника відділу, в якому трапився інцидент (залучаються на тимчасовій основі для підтримки забезпечення адміністративної, експертної і технологічної діяльності);
– зовнішніх експертів (забезпечення консультативної, експертної і технологічної діяльності).

Документація

Документація повинна містити такі елементи:

- шкалу небезпеки для класифікації інцидентів ІБ; Така шкала може складатися, наприклад, з двох положень: «небезпечно» і «безпечно». У будь-якому випадку положення шкали засноване на фактичному або передбачуваному збитку;
- форми звітів про події та інциденти ІБ, відповідні задокументовані методики та дії пов'язані з коректними процедурами використання даних і системи, сервісів і (або) мережевого резервування, планами безперервності управління;
- операційні процедури для ГРІІБ з документованими обов'язками та розподілом функцій серед призначених відповідальних осіб для ведення різних видів діяльності, наприклад таких як:

а) відключення ураженої системи, сервісу і (або) мережі, при визначених обставинах за погодженням з відповідним керівництвом і відповідно до попередньої угоди;

б) залишення ураженої системи, сервісу і (або) мережі, що знаходиться в працюючому стані;

в) ведення моніторингу потоку даних, що виходять, входять або знаходяться в межах ураженої системи, сервісу і (або) мережі;

г) активація нормальних дій і процедур планування неперервності управління та резервування згідно політиці безпеки системи, сервісу та (або) мережі;

д) ведення моніторингу та підтримка безпеки зберігання свідчень в електронному вигляді на випадок їх запиту для судового переслідування або внутрішнього дисциплінарного стягнення;

є) передача подробиць про інцидент ІБ ГРІІБ, керівництву та стороннім особам або організаціям.

Якщо можливо, документи мають бути в електронній формі (наприклад, на безпечній веб-сторінці) з посиланням на базу даних, що зберігає електронну інформацію про події/інциденти ІБ. Форма заповнюється особою, що робить повідомлення (тобто необов'язково членом ГРІІБ). Форма звіту про інциденти використовується персоналом менеджменту інцидентів ІБ, заповнюється первісною інформацією про подію ІБ, містить поточні записи оцінки інциденту та інші до повного вирішення інциденту. На кожній стадії в базу даних подій / інцидентів ІБ включаються оновлення. Запис, зроблений у базі даних, що містить «заповнену» форму або відомості про події/інциденти ІБ, потім використовується при розслідуванні інциденту.

Коригувальні та превентивні дії

Після усунення наслідків інциденту і відновлення нормального функціонування управлінських процесів, виконуються дії щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких дій проводиться аналіз ризиків, в рамках якого визначається доцільність

коригувальних і превентивних дій. В деяких випадках, якщо наслідки інциденту незначні в порівнянні з коригувальними і превентивними діями, тоді доцільно не виконувати подальших кроків після усунення наслідків інциденту.

Інструкція щодо форми звіту про події та інциденти ІБ та рекомендації щодо його заповнення

Призначенням форм звіту про події та інциденти ІБ – є забезпечення інформації про подію ІБ, а потім, якщо вона визначена як інцидент, то і про інцидент ІБ для певних осіб. Якщо працівник підозрює, що подія ІБ розвивається або вже відбулася, особливо така, яка може завдати істотних втрат або шкоди власності або репутації досліджуваного об’єкту, то він повинен негайно заповнити та передати форму звіту про подію ІБ (див. першу частину додатка А) посадовій особі відповідальній за функціонування системи управління інформаційною безпекою або безпосередньому керівнику.

Представлена інформація використовується для початку відповідного процесу оцінки, яка визначає, чи повинна ця подія бути категорована як інцидент ІБ чи ні, і в разі позитивної відповіді будуть прийняті необхідні коригувальні заходи для запобігання або обмеження втрат або шкоди. Оскільки цей процес за своїм характером є критичним по часу, то необов'язково заповнювати всі поля у формі звіту в даний момент часу. Якщо ви є членом групи забезпечення експлуатації, переглядаються вже заповнені (частково заповнені) форми, то необхідно вирішити, чи треба категорувати дану подію як інцидент ІБ. Якщо треба, то необхідно заповнити форму для інциденту ІБ якомога докладніше, направити і передати і форму для події, і інцидент ІБ ГРІБ. Незалежно від того, чи буде подія ІБ категорована як інцидент чи ні, в будь-якому випадку база даних подій/інцидентів ІБ повинна бути оновлена.

Форма інциденту ІБ повинна далі оновлюватися в міру прогресу в розслідуванні, і відповідні оновлення повинні проводитися в базі даних подій / інцидентів ІБ.

При заповненні форм виконуються наступні рекомендації:

– якщо можливо, то форми повинні заповнюватися і передаватися в електронному вигляді. Якщо існують проблеми або вважається, що існують проблеми з встановленими за замовчуванням механізмами електронного оповіщення (наприклад, електронна пошта), включаючи випадки, коли система, можливо, піддається атаці, і форми звіту можуть бути прочитані неавторизованими особами, тоді повинні використовуватися альтернативні засоби зв'язку. Альтернативними засобами зв'язку можуть бути нарочні, телефон або текстові повідомлення;

– представляйте інформацію, засновану тільки на фактах, в якій ви впевнені, нічого не придумуйте для того, щоб заповнити всі поля. Де доречно включіть інформацію, яку ви не можете підтвердити, чітко вкажіть, що це непідтверджена інформація і чому ви вважаєте, що вона вірна;

– ви повинні докладно вказати, як можна з вами зв'язатися. Дуже скоро або через деякий час може виникнути необхідність контакту з вами для подальшої інформації, що стосується вашого звіту. Якщо пізніше працівником буде виявлено, що деяка представлена інформація неточна, неповна або помилкова, то він повинен ввести поправки в звіт і надати його повторно.

У Законі «Про основні засади забезпечення кібербезпеки України» передбачено створення урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Основними її завданнями є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, що провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України, у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Забезпечення функціонування діяльності CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог чинного законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Практичне завдання:

Використовуючи інформаційні ресурси мережі Internet, навести приклад події та інциденту інформаційної безпеки довільно обраного підприємства чи організації. Заповнити форму звіту про дану подію та інцидент ІБ (Додаток А).

Теоретичні питання:

1. Що таке інцидент інформаційної безпеки?
2. Розтлумачте різницю між поняттями подія ІБ та інцидент ІБ.
3. Які ознаки інциденту інформаційної безпеки Ви знаєте?
4. Назвіть основні міжнародні та національні нормативні документи, якими визначаються процедури управління інцидентами ІБ.
5. Визначте основні етапи управління інцидентами ІБ та охарактеризуйте їх.
6. Назвіть основні завдання CERT-UA.
7. Які основні елементи повинна містити документація щодо інциденту ІБ?

Лабораторна робота №8

Ключові показники ефективності управління інцидентами інформаційної безпеки

Мета роботи – ознайомитись з ключовими показниками ефективності управління інцидентами інформаційної безпеки.

Теоретичні відомості

Для оцінки ефективності процесу управління інцидентами інформаційної безпеки необхідно визначити чіткі цільові показники, часто звані «Ключові показники ефективності» (Key Performance Indicators, KPI).

Показники, що є основою прийняття важливих рішень, називаються ключовими показниками ефективності. Ключові показники ефективності (KPI) допомагають компаніям визначити, чи вони досягають конкретних цілей. У контексті управління інцидентами цими показниками може бути кількість інцидентів, середній час розв'язання або середній час між інцидентами.

Під час відстеження KPI керування інцидентами можна виявити та діагностувати проблеми з процесами та системами, визначити орієнтири та поставити реалістичні цілі для роботи команди, а також знайти відправну точку для вирішення масштабних питань.

Припустимо, що компанія прагне вирішення всіх інцидентів протягом 30 хвилин, але вашій команді це вдається в середньому за 45 хвилин. Без конкретних показників важко зрозуміти, у чому проблема. Система оповіщення спрацьовує надто повільно? У процесі щось працює? Потрібні сучасніші діагностичні інструменти? Ця проблема пов'язана з командою чи обладнанням? (рис. 8.1).

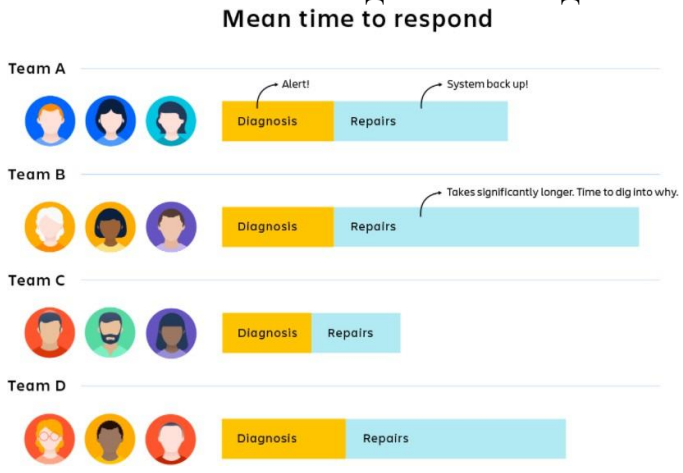

Рисунок 8.1 – Система сповіщення

Тепер додайте показники. Якщо відомо, скільки часу потрібно системі

оповіщення для спрацьовування, ви зможете зрозуміти, чи є вона причиною проблеми. Якщо діагностика займає більше половини часу, ви можете зосередитись на усуненні несправностей у ній. Якщо команда B працює на 25% повільніше, ніж команди A, C та D, можна спробувати зрозуміти, чому це відбувається.

KPI не усунуть ваші проблеми автоматично, але вони допоможуть зрозуміти суть помилок та вкажуть, куди потрібно звернути увагу та зусилля.

Відсоток відповідності SLA

Кількість інцидентів, усунених відповідно до вимог SLA у відсотках.

Відсоток оперативних рішень

Кількість інцидентів, які були усунені оперативно, у відсотках.

Кількість повторних інцидентів

Кількість ідентичних інцидентів, зареєстрованих протягом зазначеного періоду.

Відсоток повторних відкриттів

Кількість усунених інцидентів, які було відкрито повторно, у відсотках.

Невиконана робота з інцидентів

Кількість інцидентів, які чекають у черзі, щодо яких не надано рішення.

Відсоток серйозних інцидентів

Кількість серйозних інцидентів від кількості інцидентів.

Вартість однієї заявки

Середні витрати на кожну заявку.

Ступінь задоволеності кінцевими користувачами

Кількість кінцевих користувачів або клієнтів, які задоволені IT- послугами.

MTTD (середній час виявлення)

Це середній час, необхідний вашій команді, щоб виявити проблему. Цей термін часто використовується у сфері кібербезпеки командами, які зосереджені на виявленні атак та випадків несанкціонованого доступу. Якщо значення цього показника різко змінюється чи залишається недостатньо високим, варто з'ясувати причину.

MTTR

Може означати середній час виправлення, рішення, реагування чи відновлення. Мабуть, найбільшу користь становить середній час вирішення. Цей показник дозволяє зафіксувати не лише час, витрачений на діагностику та усунення безпосередньої проблеми, але й час на запобігання повторенню такої проблеми у майбутньому. Цінність цього показника найкраще виявляється під час діагностики. Чи розв’язуються інциденти так швидко та ефективно, як ви очікували? Якщо ні, потрібно з'ясувати причину, через яку час вирішення не відповідає цільовому значенню.

Час безвідмовної роботи

Це кількість часу (у відсотках), протягом якого системи доступні та

працездатні.

Практичне завдання:

1. Ознайомитися з теоретичними даними.
2. Дати розширену відповідь на питання «Чого варто боятись в аналітиці інциденту?».
3. Зробити висновки.

Теоретичні питання:

1. Перерахувати популярні KPI та метрики для управління інцидентами.
2. Навіщо потрібно визначати чіткі цільові показники?
3. Що є основою прийняття важливих рішень?
4. В чому полягає суть використання ключових показників ефективності управління інцидентами інформаційної безпеки?

Лабораторна робота №9

Розслідування інцидентів інформаційної безпеки

Мета роботи – ознайомитися з основними аспектами розслідування інцидентів інформаційної безпеки.

Теоретичні відомості

В останні роки типові захисні заходи інформаційної безпеки не можуть гарантувати повноцінного захисту інформації компанії, її інформаційних систем, сервісів, мереж та мережевого периметра. Безперечно, після впровадження методів захисту, швидше за все, залишаться вразливі місця в інформаційній інфраструктурі організації, які можуть створити передумови для шахрайських дій, що призведе до можливих інцидентів інформаційної безпеки. Більше того, з часом можуть з'являтися нові вразливості, які раніше були не ідентифіковані. Зауважимо, що інциденти ІБ можуть негативно вплинути на функціонування та діяльність компанії. Внаслідок недостатнього рівня підготовки структури до реагування на інциденти ІБ атакована організація може зазнати істотного як фінансового, так і матеріального збитку. Таким чином, організаціям, які відповідально ставляться до інформаційної безпеки, важливо застосовувати комплексний та регулярний підхід до наступного:

- виявлення та розслідування інцидентів інформаційної безпеки, надання їх експертної оцінки;
- реагування на інциденти ІБ, у тому числі активізацію необхідних додаткових захисних дій для недопущення або зменшення наслідків, а також відновлення після хакерських атак;
- набуття досвіду з інцидентів ІБ, запровадження запобіжних захисних засобів та удосконалення єдиного підходу до менеджменту комп'ютерних інцидентів.

Якою б досконалою не була система забезпечення інформаційної безпеки в організації, завжди залишається ризик. Як показує практика, організація може жодним чином не виявляти перші стадії атак, а виявляти вже лише її наслідки – втрату грошей чи недоступність того чи іншого сервісу.

Тому будь-яка подія інформаційної безпеки, яка була кваліфікована як інцидент – має розслідуватися. Без етапу розслідування не буде зроблено висновків і, як наслідок, можливо інцидент повторюватиметься надалі.

Реагування на інциденти інформаційної безпеки (ІБ) – це структурована сукупність дій, спрямована на встановлення деталей інциденту, мінімізацію збитків від інциденту та запобігання повторенню інциденту ІБ.

На практиці існує кілька фаз реагування на інцидент у сфері ІБ, а саме:

– Аналіз мережної активності. Фахівці групи реагування на інциденти інформаційної безпеки здійснюють оцінку мережевого трафіку та діагностують підозрілі інформаційні системи.

– Криміналістичний аналіз. Експерти проводять криміналістичне експрес-обстеження всіх серверів, що працюють у компанії, задіяних шахраями, з метою встановлення причин атак, переміщення атакуючих по комп'ютерних системах і мережах.

– Діагностика шкідливого коду Аналітик здійснює фундаментальний статичний та динамічний аналіз знайдених під час реагування моделей шкідливого коду. Вищезгадане дає можливість експертам виключити його закріплення у комп'ютерних системах та уникнути повторного зараження ІТ-інфраструктури компанії.

Розслідування інцидентів кібербезпеки починається з фіксації, збору та аналізу свідчень. Потім відбувається пошук відповідальних та винних осіб, а також встановлення безпосередніх причин, через які інцидент ІБ стався. Далі відбувається аналіз ІТ-інциденту, в якому також виявляють недоліки документів та методик, на основі чого створюються рекомендації щодо реагування на інциденти та налаштування захисту таким чином, щоб реагування та розслідування було можливим. Готується звіт експертизи з прикріпленими даними, який можна використовувати для розслідування інциденту інформаційної безпеки на підприємстві як самотужки, так і через інші служби.

Процес регулювання інцидентів інформаційної безпеки повинен мати певні послідовні стадії: від визначення його потреби до поширення та моніторингу. Усі процедури щодо запобігання наслідкам та першопричинам інцидентів повинні неминуче документуватися. Безперечно, документування сценаріїв реагування на кожен потенційний інцидент ІБ має проводитись експертами та фіксуватися у відповідних регламентах та правилах.

Документ, оформлений у вигляді регламенту, повинен мати такі структурні підрозділи:

– чітке формулювання подій, визначених інцидентами стосовно механізму ІБ підприємства. Наприклад, експлуатація зовнішньої електронної пошти можливо буде порушенням ІБ для державного підприємства та рядовою дією для приватної компанії;

– порядок повідомлення про подію.

Повинні бути позначені:

– формат оповіщення (усний, письмовий або за допомогою повідомлення);

– співробітники, яких потрібно повідомити;

– годинні рамки повідомлення після закінчення надходження інформації про інцидент;

– конкретні процедури щодо ліквідації результату інциденту, а також

порядок їх впровадження;

– етапи розслідування. На етапах важливо встановити відповідальних за нього співробітників, процес збору та процедуру фіксації доказів, прийнятні способи виявлення винуватця;

– процедуру притягнення до дисциплінарної відповідальності винних працівників компанії;

– дії щодо покращення безпеки, які важливо впроваджувати за результатами розслідування інциденту;

– порядок мінімізації збитків та усунення результатів інцидентів.

При підготовці регламентів важливо спиратися на розроблені методики і документацію, що довели свою корисність, наприклад, звіти, журнали.

Регламенти, які визначають механізм управління інцидентами ІБ, мають бути складовим елементом бізнес-процесів. Вони повинні позначити методи та способи класифікацій подій, та процес виявлення цих подій з подальшим внесенням до регламентуючої документації.

Практичне завдання:

1. Ознайомитися з теоретичними даними.
2. Сформулювати основні загрози інформаційної безпеки – ключові ризики.
3. Зробити висновки.

Теоретичні питання:

1. Яке головне завдання після виявлення інциденту інформаційної безпеки?
2. Стадії процесу регулювання інцидентів інформаційної безпеки.
3. Фази реагування на інцидент у сфері ІБ.
4. Охарактеризуйте процес реагування на інциденти інформаційної безпеки.

Перелік рекомендованої літератури

1. ISO/IEC 27002:2022 Information technology – Security techniques – Code of practice for information security management
2. ISO/IEC 27001:2022 Information technology. Security techniques. Information security management systems. Requirements.
3. ISO/IEC 27035:2016 Information technology - Security techniques - Information security incident management.
4. ISO/IEC 20000-2:2012 Information technology. Service management. Part 2: Code of practice.
5. Концепція розвитку телекомунікацій в Україні. Схвалено розпорядженням КМУ від 07.06.2006 р.
6. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах. – Затверджено наказом № 53 ДСТСЗІ СБУ від 04.12.2000 (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806).
7. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. – Затверджено наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р.
8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №2594-IV від 31.05.2005.
9. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. – Затверджено постановою КМУ від 29.03.2006 р. № 373.
10. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – Київ : Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190с.
11. Інформаційна безпека: навч. посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
12. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. Навчальний посібник. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
13. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
14. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010 [Електронний ресурс].— Режим доступу: http://web.ebscohost.com.
15. Салієва О. В. Когнітивна модель для дослідження рівня захищеності

об’єкта критичної інфраструктури / О. В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №2, 2020. – С. 64–73.

16. Салієва О.В. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №1, 2020. – С. 42–49.

17. Салієва О.В. Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Захист інформації. – Т. 22, №3, 2020. – С. 47–55.

18. Салієва О.В. Визначення допустимої інтенсивності зниження рівня захищеності об’єкта критичної інфраструктури ранжуванням загроз / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №2, 2020. – С. 63–76.

19. Салієва О. В. Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №3, 2020. – С. 68-75.

Додаток А

Форма для звітування про подію та інцидент інформаційної безпеки

Звіт про подію ІБ

Дата події
Номер події (назначається керівником ГРІБ):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про особу, що повідомляє:
Прізвище _____
Адреса_____
Організація_____
Телефон_____
Електронна пошта _____

Опис події ІБ

Опис події:
· Що сталося _____
· Як сталося _____
· Чому відбулося _____
· Уражені компоненти _____
· Негативний вплив на службову діяльність_____
· Будь-які ідентифіковані уразливості _____

Деталі події ІБ
Дата і час виникнення події _____
Дата і час виявлення події_____
Дата і час повідомлення про подію_____
Чи закінчилася подія? (Зазначити квадрат) так ні

Якщо «так», то уточнити, як довго тривала подія в днях / годинах / хвилинах

Звіт про інцидент ІБ

Дата інциденту
Номер інциденту (призначаються керівником ГРІБ і прив'язуються до номера (-ам) відповідних подій):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про співробітника групи забезпечення експлуатації:
Прізвище_____
Адреса_____
Телефон _____
Електронна пошта _____

Інформація про співробітника ГРІБ:
Прізвище_____
Адреса_____
Телефон _____
Електронна пошта _____

Опис інциденту ІБ

Подальший опис інциденту:
· Що сталося _____
· Як сталося _____
· Чому відбулося _____
· Уражені компоненти _____
· Негативний вплив на службову діяльність _____
· Будь-які ідентифіковані уразливості _____

Деталі інциденту ІБ:
Дата і час виникнення інциденту _____
Дата і час виявлення інциденту _____
Дата і час повідомлення про інцидент _____
Закінчився інцидент? (Зазначити квадрат) [так] [ні]
Якщо «так», то уточнити, як довго тривав інцидент в днях / годинах / хвилинах.
Якщо «ні», то уточнити, як довго він уже триває

Тип інциденту ІБ (Відмітити один квадрат, потім заповнити відповідні поля нижче):
Дійсний_____
Спроба_____
Підозра _____

Навмисна (вказати типи загрози) (один з):
Розкрадання (TH) _____
Хакерство / Логічне проникнення (HA) _____
Шахрайство (FR) _____
Неправильне використання ресурсів (MI) _____
Саботаж / фізичний збиток (SA)
Інший збиток (OD)
Шкідлива програма (MC)
Визначити:
Випадкова (вказати типи загрози) (Один з):
Відмова апаратури (HF)
Інші природні події (NE)
Відмова ПО (SF)
Визначити:
Відмова зв'язку (CF)
Втрата істотних сервісів (LE)
Пожежа (HE)
Недостатнє кадрове забезпечення (SS)
Повінь (FL)
Інші випадки (OA)
Визначити:

Помилка (вказати типи загрози) (Один з):
Операційна помилка (OE)
Помилка користувача (UE)
Помилка апаратної підтримки (HE)
Помилка конструкції (DE)
Помилка підтримки ПЗ (SE)
Інші випадки (включаючи справжні омани) (OA)
Визначити:

Невідомо
(Якщо ще не встановлений тип інциденту (навмисний, випадковий, помилка), то слід зазначити квадрат «невідомо» і, по можливості, вказати тип загрози, використовуючи скорочення, наведені вище)
Визначити:

Уражені активи
Уражені активи (якщо є)
(Дати опису активів, уражених інцидентом, або пов'язаних з ним включаючи серійні, ліцензійні номери та номери версій, по можливості)

Інформація / Дані _____
Апаратура _____
Програмне забезпечення _____
Засоби зв'язку _____
Документація_____
Негативний вплив / вплив інциденту на службову діяльність
Відзначити відповідні квадрати для зазначених нижче порушень, потім в колонці «значимість» вказати рівень негативного впливу на бізнес за шкалою 1, 10, використовуючи скорочення (покажчики категорій): (FD) - фінансові втрати / руйнування бізнес-операцій, (CE) - комерційні і економічні інтереси, (PI) - інформація, що містить персональні дані, (LR) - правові та нормативні зобов'язання (це необхідно звірити з англійським оригіналом), (MO) - менеджмент і службова діяльність, (LG) - втрата престижу (див. приклади в Додатку В). Запишіть кодові букви в колонці «вказівники», а якщо відомі дійсні вартості, то вказати їх у колонці «вартість»

	Значимість	Покажчики	Вартість
Порушення конфіденційності (тобто, несанкціоноване розкриття):			
Порушення цілісності (тобто, несанкціонована модифікація):			
Порушення доступності (тобто, недоступність):			
Порушення неспростовності			
Знищення			

Повні вартості відновлення після інциденту

	Значимість	Покажчики	Вартість
(Де можливо, необхідно вказати загальні витрати на відновлення після інциденту в цілому по шкалі 1, 10 для «значущості» і в грошах для «вартості»)			

Вирішення інциденту

Дата початку розслідування інциденту _____
Прізвище особи (осіб), що проводив (їх) розслідування інциденту

Дата закінчення інциденту _____
Дата закінчення дії _____
Дата завершення розслідування інциденту _____
Посилання та місце зберігання звіту про розслідування _____

Причетні особи (один з)

Особа (PE)
Легально заснована організація / установа (OI)
Організована група (GR)
Випадковість (AC)
Немає винного (NP)
Наприклад, природні фактори,
Відмова обладнання, помилка людини

Опис порушника
Дійсна або передбачувана мотивація (один з)

Кримінальна / фінансова вигода (CG)
Розвага / хакерство (PH)
Політика / тероризм (PT)
Реванш (RE)
Інші мотиви (OM)
Визначити:

Дії, вжиті для вирішення інциденту
(Наприклад, «ніяких дій», «підручними засобами», «внутрішнє розслідування», «зовнішнє розслідування із залученням ...»)

Дії, заплановані для дозволу інциденту
(Наприклад, див. вище)

Інші дії
(Наприклад, як і раніше потрібне проведення розслідування для іншого персоналу)

Висновок

(Відзначити один з квадратів, чи є інцидент значним чи ні і додати в короткий пояснення для обґрунтування цього висновку)

Значний
Незначний
(Вкажіть будь-які інші висновки) _____

Ознайомлені особи / суб'єкти

(Ця частина звіту заповнюється відповідною особою, на яку покладено обов'язки в області ІБ і яке формулює необхідні дії. Зазвичай цією особою є посадова особа виконкому відповідальна за функціонування системи керування інформаційною безпекою(керівник ІБ).

Керівник ІБ
Керівник ГРІБ
Місцевий керівник (уточнити, якого підрозділи)
Керівник інформаційних систем
Автор звіту
Керівник автора звіту
Представник РВ МВС(при необхідності)
Інша особа

Визначити:

Залучені особи

Ініціатор
Підпис_____
Прізвище_____
Посада_____
Дата _____

Аналітик
Підпис_____
Прізвище_____
Посада_____
Дата _____