МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

КОНСПЕКТ ЛЕКЦІЙ

для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальності 262 - «Правоохоронна діяльність»

Обговорено і рекомендовано
на засіданні кафедри кібербезпеки
та математичного моделювання
протокол № 8
від 21.01.2022р.

Чернігів – 2022

Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 – «Правоохоронна діяльність»// Укл.: Ю.М.Ткач, С.М.Семендяй - Чернігів: НУ «Чернігівська політехніка», 2022. – 133 с.

Укладачі: Ткач Юлія Миколаївна
доктор педагогічних наук, завідувач кафедри кібербезпеки та математичного моделювання, професор

Семендяй Сергій Матвійович
старший викладач кафедри кібербезпеки та математичногомоделювання

Відповідальний за випуск: Петренко Тарас Анатолійович
кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання

Рецензент: Мехед Дмитро Борисович
кандидат педагогічних наук, доцент кафедри кібербезпеки та математичного моделювання

Конспект лекцій підготовлено відповідно до навчального плану підготовки бакалаврів спеціальності 262 – Правоохоронна діяльність.

ЗМІСТ

ВСТУП

Конспект лекцій призначений для засвоєння курсу «Інформаційна безпека держави» здобувачами вищої освіти освітньо-кваліфікаційного рівня «бакалавр» спеціальності 262 – «Правоохоронна діяльність» та закріплення необхідних у подальшій роботі знань з основ інформаційної безпеки.

Матеріал дисципліни тісно пов’язаний зі спеціальними дисциплінами, що викладаються у вищих навчальних закладах технічного профілю.

У лекціях розглянуто: основні поняття, об’єкти, суб’єкти та види інформаційної безпеки; види і класифікації загроз, дестабілізуючих факторів; методів та засобів забезпечення інформаційної безпеки держави, поняття та зміст інформаційного протиборства, основи теорії інформаційної боротьби, основи безпеки інформаційних технологій та інформаційних ресурсів, способи побудови інформаційно-комунікаційних систем та мереж на основі сучасних способів передачі і обробки інформації, а також режими роботи комп’ютерних мереж. Показані основні загрози суспільству та інформаційному ресурсу України, що мають місце у нашій сучасності, розглянута система та політика забезпечення інформаційної безпеки України, викладено нормативно-правову складову процесу організації та становлення в Україні всієї структури інформаційної безпеки. Розглянуто весь комплекс нормативно-правової бази, в тому числі основні концепції, які визначають сучасний стан та подальший розвиток національної та, як її складової, інформаційної безпеки України. Наводяться нормативно-правові методи інформаційної безпеки з урахуванням вітчизняних та міжнародних стандартів.

В основу конспекту покладено матеріали багатьох відомих публікацій. Використовувалися також наукові статті та методичні розробки викладачів кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

ЛЕКЦІЯ 1. **Поняття інформаційної безпеки держави, суспільства та особи**

1. Інформаційна безпека (поняття і визначення)
2. Поняття та загальні властивості інформації. Поняття загроз
3. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері

4. Об'єкти, суб'єкти та види інформаційної безпеки
5. Співвідношення понять інформаційної та кібербезпеки

1.1. Інформаційна безпека (поняття і визначення).

Дослідження такого складного явища, як інформаційна безпека, може бути успішним лише за умови наявності розробленого понятійного апарату. Головною складовою цього апарату є система понять, завдяки яким розкриваються сутнісні моменти досліджуваного явища.

Розглянемо основні поняття, визначення і терміни.

Інформація:

1) документовані або публічно проголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі;

2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх представлення, будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Інформаційні відносини - відносини, які виникають у всіх сферах життя і діяльності держави, суспільства і людини при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційний суверенітет - здатність держави контролювати і регулювати потоки інформації поза межами держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційний простір (національний):

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та ресурсів, на яке розповсюджується юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Інформаційна інфраструктура: сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки,

виробництво інформаційних технологій, сервісного обслуговування інфраструктури і системи підготовки кадрів.

Інформаційні ресурси:

1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави у певній сфері життя чи діяльності.

Інформаційні технології:

1) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів або надання інформаційних послуг;

3) технологічний процес, предметом перероблення й результатом якого є інформація;

4) процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем;

5) система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформаційних продуктів.

Інформаційна система: організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційне середовище: усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

Інформаційний ринок: система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

Інформаційний продукт (продукція):

1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

2) документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена для задоволення потреб користувачів;

3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційне забезпечення: підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь-якої іншої діяльності у всіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційне поле:

1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту;

2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційне суспільство:

1) суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми - знань;

2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформатизація:

1) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

Інформатика: наукова діяльність, що вивчає інформаційні структури та процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, збереження і поширення (розповсюдження, реалізацію) інформації за допомогою комп'ютерної техніки.

Інформаціологія: новітня загальна фундаментальна наука про інформаційні природні процеси матеріалізації та дематеріалізації в мікро- й макроструктурах Всесвіту, що самоорганізуються.

Інформаційна війна: процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя: засоби, які дозволяють здійснювати замислені дії із повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна сфера - область діяльності, що відноситься до створення, передачі і використання інформації, включаючи особисту і суспільну свідомість, інформаційну і телекомунікаційну інфраструктуру та власне, інформацію. Інформаційна сфера – це частина соціальної діяльності суспільства, тому в ній проявляються загальні закони буття, загальні і специфічні закономірності соціального розвитку.

Інформаційна інфраструктура включає в себе:

– ***організаційні структури***, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове, фінансове забезпечення;

– ***інформаційно-телекомунікаційні структури*** - територіально розподілені державні і корпоративні комп'ютерні мережі, телекомунікаційні мережі і системи спеціального призначення та загального користування, мережі і канали передачі даних, засоби комутації і керування інформаційними потоками;

– ***телекомунікаційні технології;***

– ***системи засобів масової інформації.***

Інформаційна безпека - захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне ***інформацію*** та її ***параметри***, такі, як ***повнота, об'єктивність, доступність і конфіденційність.***

Інформаційна безпека є складовою ***національної безпеки.*** Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

Підходи до визначення поняття «інформаційна безпека»

Поняття інформаційної безпеки держави, суспільства та особи, залежно від його використання, розглядається у декількох ракурсах.

У найзагальнішому випадку інформаційна безпека - це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Більш розгорнуте формулювання інформаційної безпеки - це стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Слід відзначити, що задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок - обґрунтованість рішень та дій, що приймаються.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмету, який знаходить вираз у стійкій єдності усіх різноманітних і суперечливих формах буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Отже можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають дане утворення. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління.

Вагомість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

В інформаційному праві інформаційна безпека - це одна із сторін розгляду

інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Таким чином, визначаючи поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки в якості:

1. Стану захищеності інформаційного простору.
2. Процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет держави.
3. Стану захищеності національних інтересів держави в інформаційному середовищі.
4. Захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі.
5. До суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі.
6. Важливої функції держави.
7. Невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

1.2 Поняття та загальні властивості інформації. Поняття загроз

На сьогодні існує багато різних варіантів визначення суті терміна «інформація». Одне з визначень наступне: інформація - це зафіксоване на носії уявлення про предмети, процеси, події, явища та ін.

Під фіксацією розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове закріплення відомостей, думок. Інформація для свого функціонування завжди вимагає наявності носія.

При цьому носієм інформації може виступати поле або речовина. У деяких випадках як носій інформації може розглядатися людина. У процесі інформаційних відносин носії можуть бути або носіями-джерелами, або носіями-одержувачами залежно від напряму переміщення інформації. У Законі України «Про інформацію» під джерелами інформації розуміються передбачені, або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію. Стосовно одержувачів, то вони сприймають інформацію через той чи інший сенсор (датчик, вимірювальний перетворювач). Процес сприйняття є досить складним, включаючи процеси прийому та перетворення інформації, що забезпечує віддзеркалення об'єктивної реальності й орієнтування в навколишньому світі. Сприйняття може включати:

- виявлення об'єкта в полі сприйняття;
- розрізнення окремих ознак всередині об'єкта;
- виділення в ньому інформативного змісту, адекватного меті дії;
- формування образу сприйняття.

У наведеному вище визначенні терміна «інформація» під уявленням розуміється образ та/або суть предмета, процесу, події, природного явища тощо, сприйняті датчиками приладів або безпосередньо органами чуття, а також створені

відтворювальною і/або творчою уявою людини чи елементами штучного інтелекту різних пристроїв. При цьому уява – це психічна діяльність, що полягає у створенні уявлень і уявних ситуацій, яка в цілому не сприймалася людиною в реальній дійсності (творча уява) або відтворюють колишні враження і спогади, що спираються на життєвий досвід (відтворювальна уява). Як видно з вищевикладеного, вчені аналітично розрізняють відтворювальну й творчу уяву, але насправді ці обидва компоненти тісно взаємодіють між собою в процесі створення уявлень. Інформація має деякі істотні з погляду її захисту властивості. Ці властивості для користувача або власника інформації можна розглядати як деякі бажані стани інформації (носіїв інформації). Такими властивостями є:

– конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

– цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

– доступність - властивість інформації бути захищеною від несанкціонованого блокування.

Події, які потенційно можуть порушити одну з названих властивостей інформації, відповідно, називають загрозами порушення конфіденційності, цілісності та доступності інформації.

Загрози порушення конфіденційності спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення працездатності (доступності) спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність обчислювальної системи, або її ресурси стають недоступними.

Загрози порушення цілісності полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об’єктивних впливів зі сторони середовища експлуатації системи.

Вважають, що забезпечення безпеки інформації повинно носити комплексний характер. Усе більше фахівців пропонують свої рішення в галузі забезпечення безпеки інформаційних ресурсів як комплексні. Проте організація забезпечення безпеки інформації повинна носити не просто комплексний характер, але ще й ґрунтуватися на всебічному аналізі можливих негативних наслідків, при якому важливо не проігнорувати суттєві аспекти.

Порушення інформаційної безпеки можливе лише у випадках переміщення інформації. Наприклад, під час несанкціонованого ознайомлення (читання) документа з паперового носія відбувається переміщення (копіювання) інформації в мозок людини, яка стає носієм-одержувачем цієї інформації.

У процесі переміщення інформації може відбуватися зміна її носія. Наприклад, носіями інформації під час її переміщення можуть виступати:

– матеріальні середовища (повітря, вода, метал та ін.);

– сенсори або датчики;

– перетворювачі та інші об'єкти живої й неживої природи, що виконують функцію проміжних носіїв інформації.

Загрози *конфіденційності* спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача. Інформація зберігає

конфіденційність, якщо додержується, перш за все, режимна адекватність носіїв інформації.

Поняття «режимна адекватність» складається з термінів «режим» і «адекватність». Режим - це сукупність норм для досягнення якої-небудь мети. Наприклад, для захисту інформації. Тут обов'язково враховується режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації. Адекватність (від лат. adaequatus – прирівняний, рівний) це відповідність, правильність, точність.

Смислове значення складових поняття «режимна адекватність носіїв інформації» є таким: це відповідність режимів доступу носіїв інформації (джерела та одержувача) під час їх взаємодії.

Загрози *цілісності* інформації направлені на заборонену режимом доступу (порядком отримання, використання, розповсюдження і зберігання інформації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також внаслідок об'єктивного впливу з боку середовища, що оточує носій інформації. Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність щодо правил її модифікації (видалення).

Будь-якого суб'єкта, що впливає на носій-джерело інформації з метою модифікації інформації, можна розглядати як носія інформації, що несе в собі уявлення про необхідну модифікацію (видалення) інформації носія-джерела інформації. У процесі модифікації також відбувається переміщення інформації, що модифікується.

Вплив об'єктів, процесів зовнішнього середовища та інших чинників, які часто відносять до розряду «випадкових» - це невідповідність носія-джерела інформації встановленому режиму доступу, що часто призводить до порушення комунікабельності. Такий вплив є порушенням режимної адекватності, і як наслідок - комунікабельності носіїв інформації.

Термін «комунікабельність» (від пізньолатинського - communicabilis - той, що з’єднується) означає сумісність (здатність до спільної роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку - аналогових і дискретних, у телебаченні - з різним числом рядків розкладання телевізійного кадру тощо). Тому комунікабельні носії інформації – це носії інформації, здатні до взаємодії.

Приклад некомунікабельності носіїв: через такий сенсор, як органи зору (очі) людина не здатна сприйняти голосову (акустичну) інформацію. Приклад комунікабельності носіїв: через сенсор - органи зору (очі) людина здатна сприйняти інформацію, зафіксовану на паперовому носії зрозумілою для неї мовою.

Загрози доступності (відмова в обслуговуванні) спрямовані на навмисне або ненавмисне порушення комунікабельності носіїв інформації у процесі їх взаємодії. Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією.

Державна таємниця - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та

охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», і підлягають охороні державою.

Матеріальні носії секретної інформації - матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Система захисту державної таємниці - сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

Допуск до державної таємниці - процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій - на проведення робіт з використанням таких відомостей.

Доступ до відомостей, що становлять державну таємницю, - надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Гриф секретності - реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Засекречування відомостей та їх носіїв - введення у передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх розповсюдження.

Комерційна таємниця - відомості, що не є державними секретами, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати збитку їх інтересам.

Ступінь секретності - категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган.

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їх діяльності розробляються і за узгодженням з міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Таким чином, для державної інформації з обмеженим доступом вже визначені відомості, які в обов'язковому порядку є об'єктом захисту.

1.3 Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері

Відповідно до усталених поглядів, інтереси особистості в інформаційній сфері полягають:

− в реалізації конституційних прав людини та громадянина на доступ до

інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;

– у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають:

– у забезпеченні інтересів особистості в цій сфері;

– у зміцненні демократії;

– у створенні правової соціальної держави;

– у досягненні та підтриманні суспільного спокою;

– у духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

– для гармонійного розвитку державної інформаційної інфраструктури;

– для реалізації конституційних прав і свобод людини та громадянина в галузі одержання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності держави, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

1.4 Об'єкти, суб'єкти та види інформаційної безпеки

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особистість, колектив, суспільство, державу, світове товариство.

До суб'єктів інформаційної безпеки відносяться:

– держава, що здійснює свої функції через відповідні органи;

– громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Види інформаційної безпеки:

– особи;

– суспільства;

– держави.

Інформаційна безпека особи - це стан захищеності психіки та здоров’я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства - можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов’язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Слід зазначити, що інформаційна безпека особи та суспільства між собою тісно

пов’язані. Інформаційна безпека суспільства та його окремих осіб ***залежить від рівня:***

- інтелектуальності, спеціальної теоретичної й практичної підготовки;
- критичного мислення, морального та духовного вдосконалення;
- гармонійного розвитку особистості в суспільстві;
- технічних засобів захисту.

Інформаційна безпека держави - це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп’ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

1.5 Співвідношення понять інформаційної та кібербезпеки

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем (ІТС) і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, зрештою, до формування ***кіберпростору*** (КбП) (рис.1.1) - високорозвиненої моделі об’єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

- подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;
- розміщуються в пам’яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;
- перебувають у постійному русі по сукупності ІТ-систем і мереж.

Уперше термін «кіберпростір» було використано в Конвенції про злочинність у сфері комп’ютерної інформації від 23 листопада 2001 року. Сфера його дії на той час перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об’єктами й інтересами суб’єктів правовідносин, а також комп’ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах.

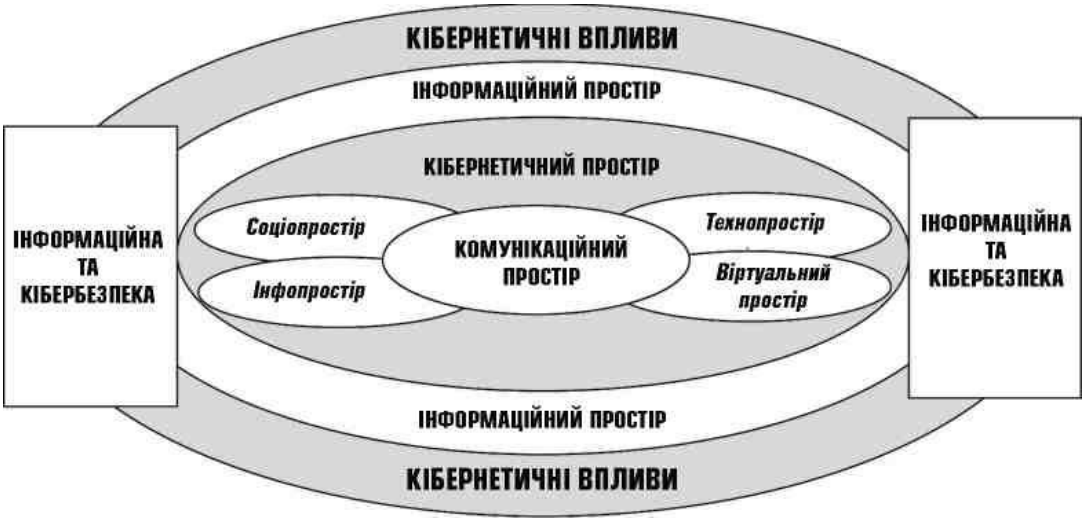

Рис. 1.1. Взаємозв’язок інформаційного та кіберпросторів

Нині кіберпростір має чимало визначень. Серед інших варто також відзначити й такі визначення поняття КбП:

– поліморфний віртуальний простір, що генерує інформаційна система (ІС) як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо);

– комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструктури - комп'ютерами, комп'ютерними мережами, програмним забезпеченням та інформаційними ресурсами, використовуване для забезпечення певних інформаційних потреб;

– штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації, що забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін електронними повідомленнями, даючи змогу із застосуванням електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

– простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, поданої у вигляді електронних комп'ютерних даних;

– об'єкти інформаційної інфраструктури що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює;

– середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Найбільш відмітними ознаками кіберпростору як субстанції, створенню якої сприяли передусім такі чинники: зміна характеру діяльності людини з ухвалення рішень; упровадження електронно-цифрових форм створення, обробки, зберігання та переміщення інформації, перехід від паперового діловодства до електронного тощо,- **абсолютна більшість фахівців** ***вважає його неперевершені можливості зі створення незлічених зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг.*** З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з ладу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сферами) і своєрідної сполученої ланки між такими поняттями, як Інтернет і кібернетика, усе це, у свою чергу, дає змогу:

– виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

– охарактеризувати злочини, втручання і загрози, пов'язані з особливостями

існування та передавання інформації;

– розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.

Сучасний стан справ зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює (рис.1.2), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

Рис. 1.2. Об’єкти впливу в інформаційному та кіберпросторі

При цьому ***інформаційну безпеку*** (ІБ) у найзагальнішому розумінні можна визначити як *такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони* (рис.1.3).

Рис. 1.3. Структура поняття «інформаційна безпека»

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об’єктів безпеки можна поділити на такі основні категорії: ***доступність*** - можливість за прийнятний час отримати певну інформаційну послугу; ***цілісність*** - актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; ***конфіденційність*** - захищеність від несанкціонованого ознайомлення.

Кібербезпеку (рис.1.4) можна визначити як *стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього*

кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам.

Рис. 1.4. Складові кібернетичної безпеки

Головні проблеми забезпечення кібернетичної безпеки постають з таких причин:

– відсутності чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави;

– дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки;

– залежності держави від програмних і технічних продуктів іноземного виробництва;

– відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки;

– дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів.

Комплексну сутність кібербезпеки за таких умов унаочнює схема, подана на рис. 1.5.

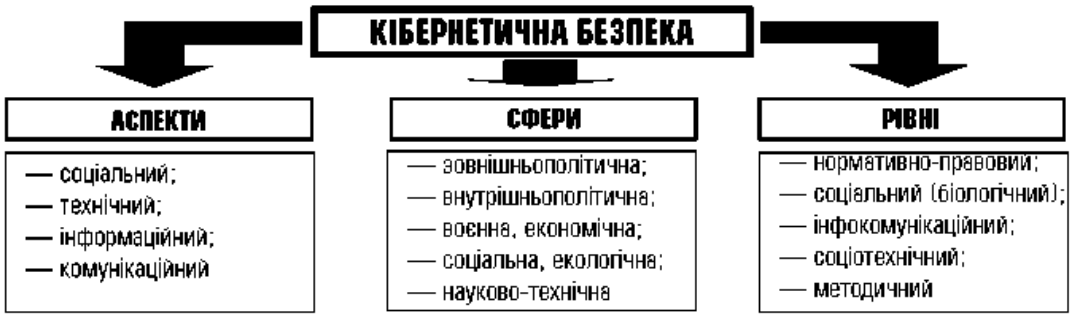

Рис. 1.5. Сутність кібернетичної безпеки

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи:

– Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV;

– Закони України «Про інформацію», «Про основи національної безпеки України», «Про Державну службу спеціального зв’язку та захисту інформації

України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»;

– Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;

– окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

Практичними кроками щодо реалізації чинної нормативно-правової бази стало створення 2007 року в складі Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім цього, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року №34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на ступінь та динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ - Департамент боротьби з кіберзлочинністю і торгівлею людьми.

ЛЕКЦІЯ 2. **Небезпеки для інформаційної безпеки держави, суспільства та особи**

1. Загрози інформаційній безпеці
2. Дестабілізуючі фактори загроз
3. Джерела загроз інформаційній безпеці

2.1 Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі і гідності і т.ін.).

Аналіз і виявлення загроз інформаційної безпеки є важливою функцією забезпечення інформаційної безпеки. Багато в чому вигляд розроблюваної системи захисту і склад механізмів її реалізації визначається потенційними загрозами, виявленими на цьому етапі. Наприклад, якщо користувачі мають доступ в Інтернет, то кількість загроз інформаційній безпеці різко зростає, відповідно, це відбивається на методах і засобах захисту і т. д.

Загроза інформаційній безпеці - це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему. Особи, які навмисно реалізують загрози, є зловмисниками.

Найчастіше загроза є наслідком наявності вразливих місць в захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення (на жаль навіть ліцензійне програмне забезпечення не позбавлене уразливостей).

Історія розвитку інформаційного середовища показує, що нові вразливі місця з'являються постійно. З такою ж регулярністю, але з невеликим відставанням, з'являються і засоби захисту. В більшості своїй засоби захисту з'являються у відповідь на виникаючі загрози, так, наприклад, постійно з'являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця. Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей проміжок часу зловмисник може завдати непоправної шкоди інформації.

У цьому зв'язку більш прийнятним є інший спосіб - спосіб попереджувального захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і потенційних загроз. Але деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками або техногенними явищами.

Знання можливих загроз інформаційній безпеці, а також вразливих місць

системи захисту, необхідне для того, щоб вибрати найбільш економічні і ефективні засоби забезпечення інформаційної безпеки.

Види загроз інформаційній безпеці

За ступенем гіпотетичної шкоди: загроза - явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системоутворюючих елементів; небезпека - безпосередня дестабілізація функціонування системи державного управління.

За повторюваністю вчинення: повторювані - такі загрози, які раніше вже мали місце; продовжувані - неодноразове здійснення загроз, що складається з ряду тотожних, які мають спільну мету.

За сферами походження: екзогенні - джерело дестабілізації системи лежить поза її межами; ендогенні - алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації: імовірні - такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, яке передує самій атаці; неможливі - такі загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай мають більше декларативний характер, не підкріплений реальною і, навіть, потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер; випадкові - такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

За джерелами походження: природного походження - включають в себе небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградацію ґрунтів чи надр, природні пожежі, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками, зміна стану водних ресурсів і біосфери тощо; техногенного походження - транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів державного управління тощо; антропогенного походження - вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення об'єкта тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (це, наприклад, може бути помилковий запуск програми, ненавмисне інсталяція закладок тощо); навмисні (інспіровані), що стали результатом навмисних дій людей (наприклад: навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо).

За значенням: допустимі - такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення; недопустимі - такі загрози, які: 1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; 2) можуть призвести до змін, не сумісних із подальшим існуванням системи.

За структурою впливу: системні - загрози, що впливають одразу на всі складові елементи суб'єкта ЗНБ; структурні - загрози, що впливають на окремі структури системи. Дані загрози є також небезпечними, водночас вони стосуються структури окремих органів державної влади або їх компонентів; елементні - загрози, що впливають на окремі елементи структури системи. Дані загрози носять постійний характер і можуть бути небезпечними лише за умови неефективності або не проведення їх моніторингу.

За характером реалізації: реальні - активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією; потенційні - активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління; здійснені - такі загрози, які втілені у життя; уявні - псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За ставленням до них: об'єктивні - такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта; суб'єктивні - така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою.

За об'єктом впливу: на державу; на людину; на суспільство.

Крім того, загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т.п.) чи відмовлення елементів обчислювальної системи, або суб'єктивну, наприклад, помилки персоналу. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними.

Отже, на будь-якому об'єкті повинні здійснюватися деякі дії чи фактори, що будуть перешкоджати реалізації конкретних захисних механізмів і заходів, створюючи тим самим відзначені вище загрози. При цьому вони будуть безпосередньо пов'язані з цими загрозами і будуть, власне кажучи, їхніми причинами. Ці події чи фактори можна охарактеризувати в такий спосіб:

– вони об'єктивно існують і можуть реалізуватися в будь-який момент часу на будь-якому об'єкті, де обробляється інформація, що підлягає захисту;

– вони не зводяться до загроз; один і той самий процес чи подія в одному випадку призводить до загроз, а в іншому не являє собою ніякої небезпеки для інформації;

– для кожного такого фактора існує можливість явно установити, з якими видами загроз він пов'язаний;

– виникає можливість здійснювати конкретні дії по протидії загрозам.

Таким чином, виявляється, що загрози виникають внаслідок здійснення цих факторів, тобто є їх результатом. Надалі ці фактори будемо називати дестабілізуючими факторами (ДФ). Як показує подальший аналіз, введення поняття ДФ цілком логічно виправдане і дозволяє одержати дуже просту, зрозумілу і наочну схему для створення моделі загроз.

2.2 Дестабілізуючі фактори загроз

Дестабілізуючі фактори - явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції ворожих держав, в яких для формування інформаційних загроз створюються і функціонують спеціальні органи і служби.

Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів відносять:

– правовий вакуум у більшості питань забезпечення інформаційної безпеки;

– навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;

– політичні конфлікти;

– зловмисні дії злочинних елементів або груп;

– відмови, збої, технічні помилки інформаційних систем (засобів);

– природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори - це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т.ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні**.**

Під політичними факторами загроз інформаційній безпеці розуміють:

– зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

– інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

– становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

– знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

– порушення інформаційних зв'язків внаслідок утворення на території колишнього СРСР нових держав;

– прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

– низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур - виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

– недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

2.3 Джерела загроз інформаційній безпеці

Виходячи з визначення загроз інформаційній безпеці, можна виділити декілька основних джерел загроз, які можуть торкатися інтересів особистості, суспільства і держави.

Джерела загроз інформаційній безпеці особистості.

Інтереси особистості, які необхідно охороняти в інформаційному суспільстві, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, а також у захисту інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навкруг неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність.

Важливою особливістю способу життя людини в інформаційному суспільстві є суттєве скорочення «інформаційних» відстаней (часу доступу до необхідної інформації), що веде до появи нових можливостей - як з формування особистості, та

і з реалізації її потенціалу. Людство впритул підходить до рубежів, за якими інформаційна інфраструктура стає, по суті, основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки.

Проблема формування розумових потреб і мотивації соціальної поведінки поки не має загального вирішення навіть для індустріального суспільства і ще більше ускладнюється стосовно інформаційного суспільства. Вона є однією з найбільш складних у сучасній психологічній науці.

В цілому структура споживчо-мотиваційної сфери особистості утворюється базовими потребами, зумовленими його генотипом (у їжі, особистій безпеці, потреба у продовженні роду, довголітті, а також потребами у спілкуванні з іншими людьми), похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб у значній мірі залежать від інформації і знань, що одержуються з навколишнього світу і, зокрема, надходять через інформаційну інфраструктуру. Спрямованість використання одержаної інформації і результати, що одержуються, визначаються, насамперед, особою людини та її духовним потенціалом.

Складність процедур, що реалізуються в сучасних технологіях доступу до необхідних інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які здійснюють розробку інформаційних технологій, визначення алгоритмів пошуку необхідної інформації, її попередньої обробки, приведення до виду, зручного для сприйняття, доведення до споживача. По суті, ці люди формують для людини інформаційний фон його життя, визначають умови, в яких він живе і діє, вирішує свої життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії людини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особистості є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, в тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що складає його особисту і сімейну таємницю, відомості про її приватне життя.

Це зумовлено, у першу чергу, труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями у мікромініатюризації засобів прихованого збирання і передавання інформації.

Джерела загроз інформаційній безпеці суспільства.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися і вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи енергетичної, транспортної, трубопровідної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації (ЗМІ) в руках невеликої групи власників.

Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування

моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності.

Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою.

Джерела загроз інформаційній безпеці держави

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

У першу чергу загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки.

Проте найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві може стати неконтрольоване розповсюдження інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна виділити наступні:

– створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника;

– маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення;

– зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень;

– дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

– провокування соціальних, політичних, національних і релігійних сутичок;

– ініціювання страйків, масових заворушень та інших акцій економічного протесту;

– ускладнення прийняття органами важливих рішень;

– підрив міжнародного авторитету держави, її співробітництва з іншими країнами;

– нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційних загроз в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється. Особливо небезпечним це є

в умовах існування майже монопольного положення компаній невеликої кількості країн на ринку інформаційних продуктів, оскільки це здатне спровокувати бажання використати наявну перевагу для досягнення тієї чи іншої політичної мети.

ЛЕКЦІЯ 3. **Методи та засоби забезпечення інформаційної безпеки держави.**

1. Принципи, покладені в основу забезпечення інформаційної безпеки держави
2. Основні форми забезпечення інформаційної безпеки держави
3. Методи забезпечення інформаційної безпеки

3.1 Принципи, покладені в основу забезпечення інформаційної безпеки держави.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, - у відповідності із законодавством. В основу забезпечення інформаційної безпеки держави повинні бути покладені наступні принципи:

- законність, дотримання балансу інтересів особистості, суспільства і держави;
- взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;
- інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

- превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки;
- адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

Превентивність (лат. praeventio від praevenio – «попереджую») зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. Оскільки це справедливо по відношенню до будь-якого виду діяльності, то можна стверджувати, що даний принцип є загальним, і його дія розповсюджується на всі сфери безпеки особистості, суспільства та держави.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі. Права та свободи суспільства в питаннях пошуку, володіння та розповсюдження інформації повинні регулюватися законодавчими актами, які видаються, щодо специфіки діяльності суспільних об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та правозастосування законодавства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації. В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони і т.ін. лежать діючі норми та принципи міждержавного права. Головним слід вважати принцип рівної безпеки. Стосовно до інформаційної сфери можна говорити про його

трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблятися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки.

Система забезпечення інформаційної безпеки держави

Забезпечення інформаційної безпеки держави - це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек. Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки.

Державна система забезпечення інформаційної безпеки країни являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є:

− виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави;

− здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

− створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

3.2 Основні форми забезпечення інформаційної безпеки держави

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права у будь-якій, в тому числі і політичній діяльності. У свою чергу, кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки своїх дій для інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного патронату та інформаційної кооперації, у другому - у формі інформаційного протиборства

Інформаційний патронат (лат. patronatys від patronys - "захисник") - форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і власне захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, - інформаційний захист.

При цьому інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація - форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі і інформаційні загрози та захист від них доступними законними способами і засобами.

Інформаційне протиборство - форма забезпечення інформаційної безпеки при здійсненні навмисних деструктивних дій суб’єктів інформаційного процесу.

Інформаційне протиборство - суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

Для конкретної особистості такими способами і засобами можуть бути:

- судовий захист прав і свобод у використанні інформації;
- адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;
- автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються.

3.3 Методи забезпечення інформаційної безпеки

Під інформаційною безпекою слід розуміти захищеність від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації або її власникам .

Завдання забезпечення інформаційної безпеки повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Існує багато методів забезпечення інформаційної безпеки:

- засоби антивірусного захисту;
- засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами;
- інструменти перевірки цілісності вмісту дисків;
- віртуальні приватні мережі;
- міжмережеві екрани;
- засоби аутентифікації користувачів;
- системи виявлення уразливостей мереж і аналізатори мережевих атак.

Кожен з перерахованих методів може бути використаний як самостійно, так і в інтеграції з іншими.

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Виявлені об'єкти можуть піддаватися лікуванню, та можуть бути видалені. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервери, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux системи, Novell).

Значно зменшують непродуктивні трудові витрати фільтри спаму, пов'язані з розбором спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників

компанії на шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси часто мають ознаки спаму і фільтруються.

Резервне копіювання є одним з основних методів захисту від втрати даних з чітким дотриманням методів зберігання копій та регулярності .

Ідентифікація та авторизація - це ключові елементи інформаційної безпеки. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування наділяє користувача певними ідентифікаційними особливостями в рамках даної мережі та визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у разі несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересиланні по електронній пошті або передачу з мережних протоколів. Завдання даного засобу захисту - забезпечення конфіденційності.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома або більше мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних. Таким чином, міжмережеві екрани значно розширюють можливості сегментування інформаційних мереж.

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної та вихідної електронної пошти. Перевірка самих поштових повідомлень і вкладень в них на основі правил, встановлених в організації, дозволяє також убезпечити компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму. Засоби тематичної фільтрації дозволяють перевіряти файли всіх поширених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відстеженні адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диску (integrity checking). Це дозволяє виявляти будь-які дії з файлами та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами.

ЛЕКЦІЯ 4. **Основи безпеки інформаційних ресурсів**

1. Загрози безпеки інформації та інформаційних ресурсів
2. Джерела загроз безпеці інформації
3. Класифікація вразливостей безпеці
4. Побудова моделі порушника
5. Забезпечення безпеки інформації та інформаційних ресурсів

4.1 Загрози безпеки інформації та інформаційних ресурсів

Насамперед заходи забезпечення інформаційної безпеки в організації спрямовуються тільки на те, щоб не допустити збитків від втрати інформації з обмеженим доступом. Відповідно до цього, вже передбачається наявність цінної інформації, в разі втрати якої організація може понести збитки. А якщо є цінна інформація, то звичайно ж є можливість здійснення будь-яких дій, які можуть нанести шкоду цій інформації. Усі шкідливі дії можуть бути здійснені тільки при наявності будь-яких слабких місць. А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити.

Виникає наступний ланцюжок: джерело загрози - фактор (вразливість) - загроза (дія) - наслідки (атака).

Джерело загрози - це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) - це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (вразливість) - це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються, програмним забезпеченням і апаратними засобами, умовами експлуатації.

Наслідки (атака) - це можливі наслідки реалізації загрози (можливі дії) при взаємодії джерела загрози через наявні фактори (вразливості).

Атака - це завжди пара "джерело-фактор", що реалізує загрозу та призводить до збитків.

Прояви збитків можуть бути різноманітні:

- моральні й матеріальні збитки ділової репутації організації;
- моральні, фізичні або матеріальні збитки, пов'язані з розголошенням персональних даних окремих осіб;
- матеріальні (фінансові) збитки від розголошення конфіденційної інформації;
- матеріальні (фінансові) збитки від необхідності відновлення порушених інформаційних ресурсів;
- матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною;
- моральні та матеріальні збитки від дезорганізації діяльності організації;
- матеріальні та моральні збитки від порушення міжнародних відносин.

Слід відзначити, що збитки можуть бути спричинені як будь-яким суб'єктом (у цьому випадку відбувається правопорушення), так і бути наслідком незалежного від суб'єкта прояву (наприклад, стихійних випадків, або інших впливів, таких як прояви техногенних властивостей цивілізації).

У першому випадку наявна вина суб'єкта, яка визначає спричинену шкоду як склад злочину, що здійснюється із злими намірами (навмисно) або по необережності, і спричинені збитки повинні класифікуватися як склад злочину, відповідно до кримінального права.

У другому випадку збитки носять імовірнісний характер і повинні бути співставленні як мінімум із тим ризиком, який обговорюється цивільним, адміністративним або арбітражним правом, як предмет розгляду. Визначення того, хто саме є причиною збитків, є другим за важливістю (після спроби цього не допустити) питанням для потерпілого.

В теорії права під **збитками** розуміють невигідні для власника майнові наслідки, що виникли внаслідок правопорушення. Збитки виражаються у зменшенні майна, або у недоодержанні прибутку, який був би одержаний при відсутності правопорушення (втрачена вигода). Якщо розглядати в якості суб'єкта, що спричинив збитки, будь-яку особистість, то категорія «збитки» є справедливою тільки у тому випадку, коли можна довести, що вони спричинені, тобто діяння особистості необхідно кваліфікувати в термінах правових актів як склад злочину. Тому при класифікації загроз безпеці інформації у цьому випадку доцільно враховувати вимоги діючого кримінального права, які визначають склад злочину.

Для прикладу можна розглянути склади злочину, які визначаються кримінальними кодексами в багатьох державах.

Крадіжка - здійснення з корисливою метою протиправного безоплатного вилучення і (або) обіг чужого майна на користь винного або інших осіб, що спричинили збитки власникові майна.

Копіювання комп'ютерної інформації - це повторювання та стійке збереження інформації на машинному або іншому носієві.

Знищення - це зовнішній вплив на майно, у результаті якого воно припиняє своє існування або приходить у повну непридатність для використання по цільовому призначенню. Знищене майно не може бути відновлене шляхом ремонту або реставрації та повністю виводиться з господарського обігу.

Знищення комп'ютерної інформації - стирання її у пам'яті комп’ютера.

Пошкодження - зміна властивостей майна, при якому суттєво погіршується його стан, втрачається значна частина його корисних властивостей і воно стає повністю або частково непридатним для цільового використання.

Модифікація комп'ютерної інформації - внесення будь-яких змін, окрім пов'язаних з адаптацією програми для комп’ютера або баз даних.

Блокування комп'ютерної інформації - штучне ускладнення доступу користувачів до інформації, не пов'язане з її знищенням.

Несанкціоноване знищення, блокування, модифікація, копіювання інформації - будь-які дії з інформацією, що не дозволені законом, власником або компетентним користувачем.

Обман (заперечення автентичності, нав'язування хибної інформації) - навмисне спотворення або приховування істини з метою введення в оману особи, у веденні

якої знаходиться майно, і таким чином домогтися від неї добровільної передачі майна, а також повідомлення з цією метою свідомо неправдивих відомостей.

Якщо розглядати в якості суб'єкта, що спричинив збитки, будь-яке природне або техногенне явище, то під збитками можна розуміти невигідні для власника майнові наслідки, викликані цими явищами, які можуть бути компенсовані за рахунок третьої сторони (страхування ризиків настання події) або за рахунок власних засобів власника інформації.

Виходячи з попередніх міркувань, можна виділити три основні види **загроз безпеці інформації:** загрози безпеці інформації при забезпеченні конфіденційності, доступності та цілісності.

Загрози безпеці інформації при забезпеченні конфіденційності:

- крадіжка (копіювання) інформації та засобів її обробки;
- втрата (ненавмисна втрата, витік) інформації та засобів її обробки.

Загрози безпеці інформації при забезпеченні доступності:

- блокування інформації;
- знищення інформації та засобів її обробки.

Загрози безпеці інформації при забезпеченні цілісності:

- модифікація (спотворення) інформації;
- заперечення автентичності інформації;
- нав'язування фальшивої інформації.

4.2 Джерела загроз безпеці інформації

Носіями загроз безпеці інформації є **джерела загроз.** Джерелами загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Причому джерела загроз можуть знаходитися як усередині організації - внутрішні джерела, так і ззовні її - зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виправданий, виходячи з попередніх міркувань стосовно вини або ризику збитку інформації, а поділ на внутрішні та зовнішні джерела виправданий тому, що для однієї й тієї ж загрози методи відбиття для внутрішніх і зовнішніх загроз можуть бути різними.

Усі джерела загроз безпеці інформації можна розділити на три групи:

- обумовлені діями суб'єкта (антропогенні джерела загроз);
- обумовлені технічними засобами (техногенні джерела загроз);
- обумовлені стихійними джерелами.

Антропогенними джерелами загроз виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорити про заподіяння збитку. Ця група джерел загроз найбільш численна та представляє найбільший інтерес з точки зору організації захисту, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи. Методи протидії у цьому випадку керовані й залежать від волі організаторів захисту інформації.

Антропогенним джерелом загроз можна вважати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що підлягає захисту. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішніми, так і внутрішніми. Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень

кваліфікації.

Внутрішні суб'єкти (джерела), як правило, являють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомих із специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного обладнання та технічних засобів мережі.

Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел складають особи з порушеною психікою та спеціально впроваджені та завербовані агенти, які можуть бути з числа основного, допоміжного та технічного персоналу, а також представників служби захисту інформації.

Друга група містить джерела загроз, що визначаються технократичною діяльністю людини та розвитком цивілізації. Проте наслідки, викликані такою діяльністю, вийшли з-під контролю людини та діють самі по собі. Людство дійсно стає все більше залежним від техніки, і джерела загроз, які залежать від властивостей техніки, менше прогнозовані і тому потребують особливої уваги. Даний клас джерел загроз безпеці інформації є особливо актуальним у сучасних умовах, оскільки очікується різке зростання числа техногенних катастроф, викликаних фізичним та моральним старінням існуючого обладнання, а також відсутністю коштів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об'єднує обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що розповсюджується на всіх. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до об'єкта захисту. Під ними розуміють, насамперед, природні катаклізми.

4.3 Класифікація вразливостей безпеці

Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через вразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформатизації.

Вразливості, властиві об'єкту інформатизації, невіддільні від нього та обумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування.

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, одержання незаконної вигоди (нанесення збитків власникові, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз з

активізації тих чи інших уразливостей, що приносять шкоду.

Кожній загрозі можуть бути зіставлені різноманітні вразливості. Усунення або суттєве послаблення уразливостей впливає на можливість реалізації загроз безпеці інформації.

Вразливості безпеці інформації можуть бути: об'єктивними, суб'єктивними, випадковими.

Об'єктивні вразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть суттєво послаблятися технічними та інженерно-технічними методами відбиття загроз безпеці інформації.

Суб'єктивні вразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.

Випадкові вразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливе тільки при проведенні комплексу організаційних та інженерно-технічних заходів із протидії загрозам інформаційній безпеці.

Моделі порушень інформаційних ресурсів

Інформаційні ресурси інформаційних систем (ІС), у першу чергу розподілені бази даних та знань є привабливими, з точки зору розташованої на них інформації, не тільки для авторизованих користувачів інформаційної системи, а також для окремих осіб або певних груп осіб, які прагнуть бути її користувачами. Ця привабливість обумовлена характером і обсягом інформації, що вводиться, обробляється, зберігається та циркулює в ІС.

Якщо та або інша особа - користувач ресурсами ІС здійснює спробу несанкціонованого (не авторизованого) доступу до інформаційних ресурсів системи (з метою: ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи тощо), то такий користувач є порушником.

Порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. Особливу небезпеку варто очікувати від зловмисних порушників, які в силу тих або інших причин перебувають під впливом:

– кримінальних осіб та їх угруповань;

– бізнесменів, комерсантів та їх об’єднань;

– політичних діячів і партій;

– агентів спецслужб інших держав, або самі входять до їх склад.

Припустимим характером дій з боку цих порушників варто вважати бажання й прагнення одержати необхідні для порушника дані для подальшого використання, модифікації або знищення з метою досягнення певних умов для себе, своїх підприємств, прихильників або конкурентів.

Крім того, необхідно враховувати, що використання ресурсів ІС, насамперед інформаційних, і їх модифікація або знищення можуть бути здійснені порушником (зловмисниками) навмисно, або ненавмисно (неправильні, непередбачені дії без злих намірів, внаслідок недбалості тощо). При цьому порушники можуть бути внутрішніми (із числа співробітників, користувачів ІС) або зовнішніми (сторонні особи чи особи, які перебувають за межами контрольованої зони, або проникли в її

межі несанкціонованим шляхом).

Кваліфікація порушника

Варто очікувати, що порушники мають певний рівень кваліфікації, достатній для успішної реалізації загроз ресурсам ІС, тобто:

– володіють інформацією щодо функціональних особливостей ІС, уміють користуватися штатними засобами;

– володіють високим рівнем знань і досвідом роботи в обслуговуванні ідентичних засобів ІС;

– володіють високим рівнем знань в галузі обчислювальної техніки й програмування на мовах розробки програмних засобів ІС, проектуванню й експлуатації подібних до ІС систем;

– володіють інформацією щодо функцій і механізмів захисту, які реалізовані як у системі захисту інформації ІС, так і у функціях і механізмах захисту, що вбудовані в базове й прикладне програмне забезпечення. За рівнем можливостей, які надаються штатною інфраструктурою інформаційної мережі, виділяють чотири рівні порушників. Класифікація ієрархічна, тобто кожний наступний рівень містить у собі функціональні можливості попереднього рівня:

– перший рівень відповідає найбільш низькому рівню можливостей порушника у системі - можливістю запуску фіксованого набору програм, які реалізують певні функції з обробки інформації;

– другий рівень визначається можливістю створення й запуску власних програм з новими функціями обробки і подальшого одержання потрібної порушнику інформації;

– третій рівень визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію технічного забезпечення інформаційної системи;

– четвертий рівень визначається інтегрованим обсягом можливостей співробітників, які здійснюють: розробку, впровадження й експлуатацію технічних засобів інформаційної системи, а також можливістю введення до складу інформаційної системи власних технічних засобів з новими функціями, щодо обробки і отримання інформації.

Ступінь ризику

Нижче наводиться приблизний перелік персоналу ІС й відповідний ступінь ризику щодо можливої реалізації загроз та нанесення шкоди залежно від зазначених робочих функцій працівників:

– найбільший ризик: системний адміністратор; адміністратор бази даних; адміністратор безпеки;

– високий ризик: оператор системи; оператор введення й підготовки даних; менеджер обробки даних; системний програміст;

– середній ризик: інженер системи; менеджер програмного забезпечення;

– обмежений ризик: прикладний програміст; інженер і оператор зв’язку; інженер по устаткуванню; оператор периферійного устаткування; бібліотекар системних магнітних носіїв; користувач-програміст; користувач-операціоніст.

– низький ризик: інженер по периферійному устаткуванню; бібліотекар магнітних носіїв користувачів.

Цілі і мета порушника:

– особиста авторизація, тобто одержати особисті легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС, з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами;

– авторизувати інших осіб, які б мали можливість одержати легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами;

– знайти прихильників або довірених осіб серед персоналу або користувачів ІС, які мають можливість одержувати легальні атрибути доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення у відповідності зі своїми намірами.

При відсутності можливості або безуспішності реалізації вищенаведених дій порушник може мати наміри:

1. Одержання атрибутів доступу авторизованих користувачів шляхом використання технічних засобів, крадіжок, купівлі, або одержання іншим шляхом.

2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІС (обчислювальних ресурсів, інформаційних ресурсів, базового й прикладного програмного забезпечення й програмного забезпечення системи технічного захисту інформації (ТЗІ), включаючи носії резервні копії, ресурсів введення/виводу інформації, телекомунікаційного устаткування, включаючи мережу передачі даних) шляхом подолання охорони або охоронної сигналізації та ін.

3. Зміни режимів функціонування ІС, її ресурсів та послуг системи.

4. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) чи інших засобів технічної розвідки (у тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для перехвату інформації.

5. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) або інших засобів (у тому числі й віддалених, наприклад в елементах комунікаційної мережі зв’язку) для генерації хибних сигналів, інформаційних символів або спотворених повідомлень.

6. Установки програмних засобів (програмних закладок або вірусів), копіювання інформації з метою її використання.

7. Установки програмних засобів (програмних закладок або вірусів) для модифікації системного програмного забезпечення, так і інформації ІС, шляхом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень з метою перевантаження систем і порушення, таким чином, доступності компонентів ІС.

8. Здійснення спроб несанкціонованого доступу до обчислювальних та інформаційних ресурсів, базового й прикладного програмного забезпечення.

9. Здійснення спроб несанкціонованого доступу до системи захисту інформації, як частини ІС, так і до її телекомунікаційної підсистеми, шляхом подолання системи управління доступом.

Рівень знань порушника

Порушник може знати:

– склад, розміщення, функціональні особливості, умови й режими функціонування елементів ІС, включаючи траси прокладених або можливих ліній зв’язку, комунікаційних мереж зв’язку й трафіки відповідних каналів передачі даних;

– порядок, засоби й режими здійснення охорони елементів ІС, місця їх розміщення і навколишню територію;

– порядок, засоби й режими здійснення організаційно-правових і технічних заходів захисту ресурсів ІС;

– основні закономірності формування в ІС баз даних і потоків запитів до них;

– за характером дій зловмисник може здійснювати: активні або пасивні дії, стосовно ресурсів і функціональних властивостей захищеності інформаційних об’єктів ІС.

Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану функціонування ІС, а під пасивною загрозою - спроба несанкціонованого проникнення в систему без зміни її стану.

За характером дій порушників можна класифікувати на:

– випадкових порушників - авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги ненавмисно, а помилково, шляхом виконання непередбачених дій з об’єктом захисту, шляхом випадкового подолання засобів управління доступом тощо;

– терплячих зловмисників - авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою схованого подолання засобів управління доступом тощо;

– рішучих зловмисників, які мають на меті порушити ту або іншу властивість інформації. Зловмисники прагнуть перебороти: засоби організаційного обмеження доступу, охоронної сигналізації, керування доступом до фізичних ресурсів, елементи будівельних конструкцій, тощо і одержати можливість фізичного доступу до засобів обробки, зберігання або передачі інформаційних ресурсів з метою виводу їх з ладу, зміни режимів функціонування, крадіжки носіїв інформації та ін.;

– зловмисників, які використовують засоби віддаленого доступу до інформаційних об’єктів з умов: витоку інформації технічними каналами, реалізації спеціальних впливів на інформацію з технічних каналів, впливу на мережне устаткування локальних або розподілених мереж, у тому числі й засоби телекомунікаційних мереж (АТС і лінії зв’язку), які використовуються елементами ІС.

Дії порушників можуть бути спрямованими на порушення функціональних властивостей захищеності інформаційних об’єктів, зокрема на порушення:

– конфіденційності, цілісності й доступності інформаційних об'єктів;

– функцій спостереження за діяльністю користувачів і процесів, однозначної ідентифікації користувачів, ресурсів і процесів.

Така класифікація дає можливість чітко визначити методи та засоби запобігання несанкціонованим діям порушників, а також визначити організаційно-правові заходи, які потрібні для побудови комплексної системи захисту інформації.

Порушники можуть використовувати такі методи та засоби:

– агентурні методи одержання відомостей через підкуплених користувачів і персонал, а також через прихильників чи довірених осіб з числа штатних працівників або таких, які мають доступ до ресурсів ІС;

– пасивні технічні засоби перехоплення інформаційних сигналів;

– штатні засоби ІС або недоліки проектування системи захисту інформації від несанкціонованого доступу (НСД);

– методи й засоби активного впливу на елементи ІС, які змінюють конфігурацію ІС (підключення додаткових або модифікація штатних технічних засобів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ і т.п.).

За місцем здійснення порушень дії зловмисника можна класифікувати:

– без одержання доступу на контрольовану територію із використанням технічних засобів віддаленого доступу через засоби: Internet, електронної пошти, модемного зв’язку чи дистанційної розвідки (наприклад: по оптичних, акустичних каналах, каналах побічних електромагнітних випромінювань і т. ін.), або з використанням засобів одержання інформації з мережі передачі даних (наприклад: шляхом підключення або «врізання» у лінії зв’язку);

– з одержанням доступу на контрольовану територію ІС або до робочих місць кінцевих користувачів, але без доступу до технічних засобів ІС, також з використанням технічних засобів дистанційної розвідки з подальшим несанкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІС;

– з одержанням доступу до робочих місць кінцевих користувачів ІС з подальшим несанкціонованим доступом до пристроїв введення/виводу інформації, копіювання, до канального або устаткування, яке утворює канал й до інших елементів ІС;

– з одержанням доступу до засобів управління ІС і засобів управління комплексною системою захисту інформації з подальшими розширеними можливостями доступу до ресурсів ІС та послуг системи.

4.4 Побудова моделі порушника

Для подальшої організації надійного захисту інформації організації повинні не тільки оцінити весь спектр можливих погроз, але й спробувати виявити категорії порушників і ті методи, які вони використовують.

Розглянемо тепер модель порушника. Порушник (user violator) - користувач, який здійснює несанкціонований доступ до інформації. Оскільки під порушником розуміється людина, то цілком зрозуміло, що створення його формалізованої моделі - дуже складне завдання. Тому, звичайно, мова може йти тільки про неформальну або описову модель порушника.

Зазначимо, що існує визначення: хакер (hacker) і кракер (cracker). Основна відмінність складається в постановці цілей злому комп'ютерних систем: перші ставлять дослідницькі задачі по оцінці та знаходженню слабких місць з метою подальшого підвищення надійності комп'ютерної системи. Кракери виконують вторгнення в систему з метою руйнування, крадіжки, псування, модифікації інформації та роблять правопорушення з корисливими намірами швидкого збагачення. Але ці два поняття зводяться до одного поняття - порушник.

Порушник - це особа, яка може отримати доступ до роботи з включеними до складу ІС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

В кожному конкретному випадку для кожного об'єкта визначаються імовірні загрози і моделі потенційних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки (СБ) вимагається для кожного об'єкта вибрати з кількох можливих типів порушників один, на який і буде орієнтована СБ, що проектується.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він має);

– припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що за своїм рівнем порушник - це фахівець вищої кваліфікації, який має повну інформацію про систему.

Звичайно розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи:

– зовнішні;

– внутрішні порушники.

Серед зовнішніх порушників виділяють такі:

– добре озброєна й оснащена силова група, що діє ззовні швидко і напролом;

– поодинокий порушник, що не має допуску на об'єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають перед ним переваги.

Серед потенційних внутрішніх порушників можна відзначити:

– допоміжний персонал об'єкта, що допущений на об'єкт, але не допущений до життєво важливого центру ІС;

– основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

– співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливості для збору необхідної інформації і вчинення акції.

Має також розглядатися можливість змови між порушниками різних типів, що ще більше ускладнює задачу формалізації моделей порушника.

Але слід відзначити, що такий поділ є дуже загальним, а також не всі групи мають важливе значення для всіх ІС.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

– користувачі (оператори) системи;

– персонал, що обслуговує технічні засоби (інженери, техніки);

– співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти);

– технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІС);

– співробітники служби безпеки;

– керівники різних рівнів та посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

– клієнти (представники організацій, громадяни);

– відвідувачі (запрошені з якого-небудь приводу);

– представники організацій, що займаються забезпеченням життєдіяльності організації (енерго-, водо-, теплопостачання і т. ін.);

– представники конкуруючих організацій (іноземних служб) або особи, що діють за їхнім завданням;

– особи, які випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку);

– будь-які особи за межами контрольованої зони.

Можна виділити також три основні мотиви порушень:

– безвідповідальність;

– самоствердження;

– з корисною метою.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково здійснює руйнівні дії, які не пов'язані, проте, зі злим умислом. У більшості випадків - це наслідок некомпетентності, недбалості або невдоволення.

Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру «користувач - проти системи» заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІС може бути викликане корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до інформації в ІС. Навіть якщо ІС має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Усіх порушників можна класифікувати за рівнем знань про ІС:

– знає функціональні особливості ІС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

– має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

– має високий рівень знань у галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

– знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

– застосовує суто агентурні методи отримання відомостей;

– застосовує пасивні засоби (технічні засоби перехоплення без модифікації

компонент системи);

– використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;

– застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

– у процесі функціонування (під час роботи компонент системи);

– у період коли система неактивна (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т. д.);

– як у процесі функціонування, так і в період коли компонент системи неактивний.

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути охарактеризований згідно з класифікаціями, наведеними вище. Всі значення характеристик мають бути оцінені (наприклад, за 5-бальною системою) і зведені до відповідних форм.

Однак при формуванні моделі порушника на її виході обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення і відомості про порушення.

Слід звернути увагу на те, що всі злочини, зокрема і комп'ютерні, здійснюються людиною. Користувачі АС є її складовою, необхідним елементом. З іншого ж боку, вони є основною причиною і рушійною силою порушень і злочинів. Отже, питання безпеки захищених АС фактично є питанням людських відносин та людської поведінки.

4.5 Забезпечення безпеки інформації та інформаційних ресурсів

Напрями забезпечення безпеки інформації - це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особистості.

З урахуванням практики, що склалася на теперішній час, виділяють наступні **напрями захисту інформації**:

– правовий захист - це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;

– організаційний захист - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, яка виключає або послаблює нанесення будь-яких збитків виконавцям;

– інженерно-технічний захист - це використання різноманітних технічних засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інформації, можуть бути охарактеризовані цілим рядом параметрів, що відображають, окрім напрямів, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх розповсюдження, охоплення та масштабність.

Так, за характером загроз заходи захисту орієнтовані на захист інформації від розголошення, витоку та несанкціонованого доступу. За способом дії їх можна поділити на попередження, виявлення, припинення та відновлення збитків або інших утрат. За охопленням заходи захисту можуть розповсюджуватися на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури. Масштабність заходів захисту характеризується як об'єктовий, груповий або індивідуальний захист.

Правовий захист

Поняття **права** визначається як сукупність загальнообов'язкових правил і норм поведінки, які встановлені або санкціоновані державою, по відношенню до певних сфер життя та діяльності державних органів, підприємств (організацій) та населення (окремої особистості).

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.

У нашій державі такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладене у відповідних кодексах. Що стосується відомчих нормативних актів, то вони визначаються наказами, керівництвами та інструкціями, які видаються відомствами, організаціями та підприємствами, що діють у межах певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу та змісту, співвіднесення його зі всією системою законів та правових актів України.

Вимоги інформаційної безпеки повинні органічно входити до усіх рівнів законодавства, у тому числі й у конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні закони, відомчі правові акти і т.і. Звичайно використовується наступна структура правових актів, які орієнтовані на правовий захист інформації.

– **Конституційне законодавство** - норми, що стосуються питань інформатизації та захисту інформації, входять до нього як складові елементи.

– **Загальні закони,** кодекси (про власність, про надра, про права громадян, про громадянство, про податки, про антимонопольну діяльність і т.ін.), які включають норми з питань інформатизації та інформаційної безпеки.

– **Закони про організацію управління** стосовно окремих структур господарства, економіки, системи державних органів та визначення їхнього статусу. Такі закони включають окремі норми з питань захисту інформації. Поряд із загальними питаннями інформаційного забезпечення та захисту інформації конкретного органу ці норми повинні встановлювати його обов'язки з формування, актуалізації та безпеки інформації, що представляє загальнодержавний інтерес.

– **Спеціальні закони**, які відносяться до конкретних сфер відносин, галузей господарства, процесів. До їхнього числа входять Закони України «Про інформацію», «Про захист інформації в автоматизованих системах» і т.ін. Власне склад і зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

– **Підзаконні нормативні акти** із захисту інформації.

– **Правоохоронне законодавство України**, яке містить норми про відповідальність за правопорушення у сфері інформатизації.

Спеціальне законодавство в галузі безпеки інформації може бути представлене сукупністю законів. В їхньому складі особливе місце займають Закони «Про інформацію» та «Про захист інформації в автоматизованих системах», які закладають основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

– інформації та інформаційних систем;

– суб'єктів - учасників інформаційних процесів;

– правовідносин виробників та споживачів інформаційної продукції;

– власників (джерел) інформації - обробників та споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян та держави.

Ці закони також визначають основи захисту інформації у системах обробки і при її використанні з урахуванням категорій доступу до відкритої інформації і до інформації з обмеженим доступом. Ці закони містять, крім того, загальні норми з організації та ведення інформаційних систем, включаючи банки даних державного призначення, порядок державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту та гарантій прав учасників інформаційного процесу.

Питання правового режиму інформації з обмеженим доступом реалізуються у двох самостійних законах про державну та комерційну (проект) таємниці.

Таким чином, правовий захист інформації забезпечується нормативно-законодавчими актами, сукупність яких за рівнем представляє ієрархічну систему від Конституції України до функціональних обов'язків і контрактів конкретного виконавця, які визначають перелік відомостей, що підлягають охороні, і заходи відповідальності за їх розголошення.

Одним із нових напрямків правового захисту є страхове забезпечення. Воно призначене для захисту власної інформації та засобів її обробки як від традиційних загроз (крадіжки, стихійні лиха), так і від загроз, що виникають у ході роботи з інформацією. До них відносяться розголошення, витік та несанкціонований доступ до конфіденційної інформації.

Метою страхування є забезпечення страхового захисту фізичних та юридичних осіб від страхових ризиків у вигляді повного або часткового відшкодування збитків і втрат, які спричинені стихійними лихами, надзвичайними подіями в різних галузях діяльності, протиправними діями з боку конкурентів та зловмисників шляхом виплати грошової компенсації або надання сервісних послуг (ремонт, відновлення) при настанні страхової події.

Опираючись на державні правові акти та враховуючи відомчі інтереси на рівні конкретного підприємства (фірми, організації), розроблюються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких

документів відносяться:

- положення про збереження конфіденційної інформації;
- перелік відомостей, які складають конфіденційну інформацію;
- інструкція про порядок допуску співробітників до відомостей, які складають конфіденційну інформацію;
- положення про спеціальне діловодство та документообіг;
- перелік відомостей, які дозволені до опублікування у відкритому друці;
- положення про роботу з іноземними фірмами та їхніми представниками;
- зобов'язання співробітника про збереження конфіденційної інформації;
- пам'ятка співробітнику про збереження комерційної таємниці.

Наведені вище нормативні акти спрямовані на попередження випадків неправомірного оголошення (розголошення) секретів на правовій основі - у випадку їх порушення повинні прийматися відповідні заходи впливу.

Залежно від характеру інформації, її доступності для зацікавлених споживачів, а також економічної доцільності конкретних захисних заходів, можуть бути обрані наступні форми захисту інформації:

- патентування;
- авторське право;
- признання відомостей конфіденційними;
- товарні знаки;
- застосування норм зобов'язального права.

Існує певна різниця між авторським, правом та комерційною таємницею. Авторське право захищає тільки форму вираження ідеї. Комерційна таємниця відноситься безпосередньо до змісту. Авторське право захищає від копіювання незалежно від конфіденційних відносин із власником. До авторського права вдаються при широкій публікації своєї інформації, у той час як комерційну таємницю тримають у секреті. Очевидно, що порівняно з патентом та авторським правом комерційна таємниця та виробнича таємниці є найбільш зручними, надійними та гнучкими формами захисту інформації.

Окрім вищевикладених форм правового захисту та права належності інформації знаходить широке розповсюдження офіційна передача права на користування нею у вигляді ліцензії.

Ліцензія (від лат. licentia – «свобода, право») - це дозвіл, виданий державою на проведення деяких видів господарської діяльності, включаючи зовнішньоторговельні операції (ввезення та вивезення) та надання права використовувати захищені патентами винаходи, технології, методики. Ліцензійні дозволи надаються на певний час і на певні види товарів.

Комерційна таємниця - це відомості, які не є державними секретами, пов'язані з виробництвом, технологією, управлінням, фінансами та іншою діяльністю, розголошення, витік та несанкціонований доступ до якої може призвести до збитків їхнім власникам.

До комерційної таємниці не відносяться:

- відомості, що охороняються державою;
- відомості, які є загальновідомими на законній підставі;
- відомості про негативні сторони діяльності;

– установчі документи та відомості про господарську діяльність.

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які наступні претензії до несумлінного співробітника, клієнта, конкурента та посадової особи будуть просто безпідставними.

Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений до виконання посадових обов'язків) у письмовому вигляді, то співробітник, який викрав важливу інформацію при порушенні встановленого порядку роботи з нею скоріше всього не буде покараний.

Правові норми забезпечення безпеки та захисту інформації на конкретному підприємстві (фірмі, організації) відображаються у сукупності установчих, організаційних та функціональних документів.

Вимоги забезпечення безпеки та захисту інформації відображаються у Статуті (установчому договорі) у вигляді наступних положень:

– підприємство має право визначати склад, обсяги та порядок захисту конфіденційних відомостей, вимагати від своїх співробітників забезпечення їх збереження та захисту від внутрішніх та зовнішніх загроз;

– підприємство зобов'язане забезпечувати збереження конфіденційної інформації.

Такі вимоги дають **адміністрації підприємства наступні права**:

– створювати організаційні структури із захисту конфіденційної інформації;

– видавати нормативні та розпорядчі документи, які визначають порядок виділення відомостей конфіденційного характеру та механізми їхнього захисту;

– включати вимоги із захисту інформації в угоди з усіх видів діяльності;

– вимагати захисту інтересів підприємства з боку державних інстанцій;

– розпоряджатися інформацією, що є власністю підприємства, з метою вигоди та недопущення економічних збитків колективу підприємства та власникові засобів виробництва;

– розробляти «Перелік відомостей конфіденційної інформації».

Організаційний захист — це регламентація виробничої діяльності та взаємовідносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояву внутрішніх та зовнішніх загроз.

Організаційний захист забезпечує:

– організацію режиму, охорони, роботу з кадрами, з документами;

– використання технічних засобів безпеки та інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз діяльності підприємства (організації).

Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей у значній мірі обумовлюються не технічними аспектами, а зловмисними діями та недбалістю користувачів або персоналу. Впливу цих аспектів практично неможливо запобігти за допомогою технічних заходів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних

заходів, які вилучали б (або зводили до мінімуму) можливість виникнення небезпеки конфіденційності інформації.

До **основних організаційних заходів** зазвичай відносять наступні:

– організація режиму та охорони - їх мета:

– виключення можливості таємного проникнення на територію та у приміщення сторонніх осіб;

– забезпечення зручності проходу та переміщення співробітників та відвідувачів;

– створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу;

– контроль та дотримання часового режиму праці та перебування на території персоналу підприємства;

– організація та підтримка надійного пропускного режиму та контролю співробітників і відвідувачів і т.ін.;

– організація роботи із співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення із співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з мірою відповідальності за порушення правил захисту інформації;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів і носіїв конфіденційної інформації, їх облік, використання, повернення, зберігання та знищення;

– організація використання технічних засобів збирання, обробки, нагромадження та зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційній інформації та розробка заходів із забезпечення її захисту;

– організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму та зміст, які спрямовані на забезпечення безпеки інформації в конкретних умовах.

Особливості організаційного захисту комп'ютерних інформаційних систем

Організація захисту комп'ютерних інформаційних систем та мереж визначає порядок і схему функціонування основних їхніх підсистем, використання пристроїв та ресурсів, взаємовідносини користувачів між собою відповідно з нормативно-правовими вимогами та правилами. Захист інформації на основі організаційних заходів відіграє значну роль у забезпеченні надійності та ефективності, оскільки несанкціонований доступ та витік інформації найчастіше зумовлені зловмисними діями, недбалістю користувачів або персоналу. Ці фактори практично неможливо виключити або локалізувати за допомогою апаратних і програмних засобів, криптографії та фізичних засобів захисту, тому сукупність організаційних, організаційно-правових та організаційно-технічних заходів, які застосовуються разом із технічними методами, мають за мету виключити, зменшити або повністю усунути збитки при дії різноманітних деструктивних факторів.

Організаційні засоби захисту комп'ютерних інформаційних систем та мереж найчастіше застосовуються у наступних випадках:

– при проектуванні, будівництві та обладнанні приміщень, вузлів мереж та інших об'єктів інформаційної системи для виключення впливу стихійного лиха, можливості недозволеного проникнення у приміщення і т.ін.;

– при підборі та підготовці персоналу - в цьому випадку передбачається перевірка осіб, які приймаються на роботу, створення умов, при яких персонал був би зацікавлений у збереженні інформації, навчання правилам роботи із закритою інформацією, ознайомлення з мірою відповідальності за порушення правил захисту і т.ін.;

– при зберіганні та використанні документів та інших носіїв (маркування, реєстрація, визначення правил видачі та повернення, ведення документації і т.ін.);

– при дотриманні надійного пропускного режиму до технічних засобів комп'ютерних мереж та систем при роботі змінами (призначення відповідальних за захист інформації у змінах, контроль за роботою персоналу, ведення автоматизованих журналів роботи, знищення встановленим порядком закритих виробничих документів);

– при внесенні змін у програмне забезпечення (суворе санкціонування, розгляд та затвердження проектів змін, перевірка їх на задоволення вимог захисту, документальне оформлення змін і т.ін.);

– при підготовці та контролі роботи користувачів.

Служба захисту інформації

Одним із найважливіших організаційних заходів є створення спеціальних штатних служб захисту інформації у закритих інформаційних системах у вигляді адміністратора безпеки мережі та адміністратора безпеки розподілених баз та банків даних, які містять відомості конфіденційного характеру.

Цілком очевидно, що організаційні заходи повинні чітко плануватися, спрямовуватися та здійснюватися певною організаційною структурою, певним спеціально створеним для цих цілей структурним підрозділом, укомплектованим відповідними фахівцями з безпеки діяльності та захисту інформації.

Найчастіше таким структурним підрозділом є **служба безпеки підприємства** (фірми, організації), на яку покладаються **наступні функції**:

– організація та забезпечення охорони персоналу, матеріальних та фінансових цінностей та захисту конфіденційної інформації;

– забезпечення пропускного та внутрішньо об’єктового режиму на території, в будівлях та приміщеннях, контроль дотримання вимог режиму співробітниками, суміжниками, партнерами та відвідувачами;

– керівництво роботами з правового та організаційного регулювання відносин із захисту інформації;

– участь у розробці основоположних документів з метою закріплення в них вимог забезпечення безпеки та захисту інформації, а також положень про підрозділи, трудові договори, угоди, підряди, посадові інструкції та обов'язки керівництва, спеціалістів, робітників та службовців;

– розробка та здійснення разом з іншими підрозділами заходів із забезпечення роботи з документами, що містять конфіденційні відомості; при всіх видах робіт

організація та контроль виконання вимог «Інструкції із захисту конфіденційної інформації»;

– вивчення усіх сторін виробничої, комерційної, фінансової та іншої діяльності для виявлення та наступної протидії будь-яким спробам нанесення збитків, ведення обліку та аналіз порушень режиму безпеки, накопичення та аналіз даних про зловмисні прагнення конкурентної та інших організацій, про діяльність підприємства та його клієнтів, партнерів, суміжників;

– розробка, ведення, оновлення та поповнення "Переліку відомостей, що носять конфіденційний характер" та інших нормативних актів, які регламентують порядок забезпечення та захисту інформації;

– забезпечення суворого виконання вимог нормативних актів із забезпечення виробничих секретів підприємства;

– здійснення керівництва службами та підрозділами безпеки підвідомчих підприємств, організацій, закладів та іншими структурами;

– організація та регулярне проведення обліку співробітників підприємства та служби безпеки з усіх напрямів захисту інформації та забезпечення безпеки виробничої діяльності;

– ведення обліку та суворого контролю виділених для конфіденційної роботи приміщень, технічних засобів у них, що мають потенційні канали витоку інформації та канали проникнення до джерел інформації, які знаходяться під охороною;

– забезпечення проведення всіх необхідних заходів із припинення спроб нанесення моральних та матеріальних збитків з боку внутрішніх та зовнішніх загроз;

– підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств для вивчення криміногенної обстановки в районі (зоні) та надання взаємної допомоги в кризових ситуаціях.

Служба безпеки є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівникові підприємства. Очолює службу безпеки начальник служби безпеки у посаді заступника керівника підприємства з безпеки.

Організаційно *служба безпеки* може складатися з наступних *структурних одиниць:*

– підрозділу режиму та охорони;

– спеціального підрозділу з обробки документів конфіденційного характеру;

– інженерно-технічних підрозділів;

– інформаційно-аналітичних підрозділів.

У такому складі служба безпеки здатна забезпечити захист конфіденційної інформації від будь-яких загроз.

На *служби безпеки* покладаються наступні *завдання*:

– визначення кола осіб, які відповідно до положення, яке вони займають на підприємстві, прямо чи непрямо мають доступ до відомостей конфіденційного характеру;

– визначення ділянок зосередження конфіденційних відомостей;

– визначення кола сторонніх підприємств, зв'язаних із даним підприємством кооперативними зв'язками, на яких у силу виробничих відносин можливий вихід з-під контролю відомостей конфіденційного характеру;

– виявлення кола осіб, не допущених до конфіденційної інформації, але які проявляють підвищений інтерес до таких відомостей;

– виявлення кола підприємств, у тому числі іноземних, що зацікавлені у доступі до відомостей, які охороняються, з метою нанесення економічних збитків даному підприємству, усунення економічного конкурента або його компрометації;

– розробка системи захисту документів, що містять відомості економічного характеру;

– визначення на підприємстві ділянок, уразливих в аварійному відношенні, вихід із ладу яких може нанести матеріальні збитки підприємству та зірвати поставки готової продукції або комплектуючих підприємствам;

– визначення на підприємстві технологічного обладнання, вихід (або виведення) якого з ладу може призвести до великих економічних втрат;

– визначення та обґрунтування заходів правового, організаційного та інженерно-фізичного захисту підприємства, персоналу, продукції та інформації;

– розробка необхідних заходів, спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки;

– впровадження в діяльність підприємства новітніх досягнень науки та техніки, передового досвіду у галузі забезпечення економічної та інформаційної безпеки;

– організація навчання співробітників служби безпеки відповідно до їх функціональних обов'язків;

– вивчення, аналіз та оцінка стану забезпечення економічної та інформаційної безпеки підприємства та розробка пропозицій та рекомендацій для його удосконалення;

– розробка техніко-економічних обґрунтувань, спрямованих на придбання технічних засобів, одержання консультації у спеціалістів, розробку необхідної документації з метою удосконалення системи заходів із забезпечення економічної та інформаційної безпеки.

Організаційні заходи є вирішальною ланкою формування та реалізації комплексного захисту інформації та створення системи безпеки підприємства.

Інженерно-технічний захист - це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації.

Основне завдання інженерно-технічного захисту - це попередження розголошення, витоку, несанкціонованого доступу та інших форм незаконного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об'єктів захисту та заходів, що проводяться, передбачають розгляд деякої системи класифікації засобів інженерно-технічного захисту за видом, орієнтацією та іншими характеристиками.

Наприклад, засоби інженерно-технічного захисту можна класифікувати за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким здійснюється протидія з боку служби безпеки.

За функціональним призначенням засоби інженерно-технічного захисту поділяються на наступні групи: фізичні засоби захисту, апаратні засоби захисту, програмні засоби захисту, криптографічні засоби захисту.

Фізичні засоби включають різноманітні пристрої та споруди, які

перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних носіїв, фінансів та інформації від протиправних дій.

До **апаратних засобів** відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне завдання апаратних засобів - забезпечення стійкого захисту від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

Програмні засоби охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різноманітного призначення та засобах обробки (збирання, нагромадження, зберігання, обробки та передачі) даних.

Криптографічні засоби - це спеціальні математичні та алгоритмічні засоби захисту інформації, що передається системами та мережами зв'язку, зберігається та обробляється на ЕОМ із використанням різноманітних методів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розповсюдження. Проте із-за того, що вони не мають достатньої гнучкості, часто втрачають свої захисні властивості при розкритті принципу їхньої дії і в подальшому не можуть бути використані.

Програмні методи та засоби більш надійні, період їхнього гарантованого використання значно більший, ніж апаратних методів та засобів.

Криптографічні методи та засоби займають важливе місце і є надійним засобом забезпечення захисту інформації на тривалі періоди.

Очевидно, що такий поділ засобів захисту інформації достатньо умовний, оскільки на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгоритмів закриття інформації.

Фізичні засоби захисту - це різноманітні пристрої, конструкції, апарати, вироби, призначені для створення перепон на шляху руху зловмисників.

До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для заборони несанкціонованого доступу (входу, виходу), пронесення (винесення) засобів і матеріалів та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення наступних завдань:

- охорона території підприємства та спостереження за нею;
- охорона будівель, внутрішніх приміщень та контроль за ними;
- охорона обладнання, продукції, фінансів та інформації;
- здійснення контрольованого доступу до будівель та приміщень.

Усі фізичні засоби захисту об'єктів можна розділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. Охоронна сигналізація та охоронне телебачення, наприклад, відносяться до засобів виявлення загроз; загорожі навколо об'єктів - це засоби попередження несанкціонованого проникнення на територію, а підсилені двері, стіни, стелі, грати на вікнах та інші заходи служать захистом також і від проникнення, і від інших злочинних дій (підслуховування, обстрілу, кидання гранат і т.ін.). Засоби пожежогасіння відносяться до систем ліквідації загроз.

У загальному випадку за фізичною природою та функціональним призначенням усі засоби цієї категорії можна поділити на наступні групи:

– охоронні та охоронно-пожежні системи;

– охоронне телебачення;

– охоронне освітлення;

– засоби фізичного захисту.

До засобів фізичного захисту відносяться:

– природні та штучні перепони (бар'єри);

– особливі конструкції периметрів, проходів, віконних та дверних плетінь, приміщень, сейфів, сховищ і т.ін.;

– зони безпеки.

Природні та штучні бар'єри призначені для протидії незаконному проникненню на територію об'єкта. Проте основне захисне навантаження лягає все ж таки на штучні бар'єри, такі як паркани та інші види огорож. Практика показує, що огорожі складної конфігурації здатні затримати зловмисника на достатньо тривалий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих огорож, які здійснюють певний вплив відлякування на порушника.

Особливі конструкції периметрів, проходів, віконних сплетінь, приміщень, сейфів, сховищ є обов'язковими з точки зору безпеки для будь-яких організацій та підприємств. Ці конструкції повинні протистояти будь-яким способам фізичного впливу з боку кримінальних елементів:

– механічним деформаціям, руйнуванню свердлінням, термічному та механічному різанню, і т.ін.;

– несанкціонованому доступу шляхом підробки ключів, відгадування коду і т.ін.

Одним із головних технічних засобів захисту проходів, приміщень, сейфів та сховищ є замки. Вони бувають простими (з ключами), кодовими (у тому числі з часовою затримкою на відкривання) і з програмним пристроями, що відкривають двері та сейфи в певний час.

Важливим засобом фізичного захисту є планування об'єкта, його будівель та приміщень за зонами безпеки, які враховують міру важливості різних частин об'єкта з точки зору нанесення збитків від різного виду загроз. Оптимальне розташування зон безпеки та розташування в них ефективних технічних засобів виявлення, відбиття та ліквідації наслідків протиправних дій складає основу концепції інженерно-технічного захисту об'єкта.

Зони безпеки повинні розташовуватися на об'єкті послідовно, від огорожі навкруг території об'єкта до сховищ цінностей, створюючи ланцюг перешкод (рубежів), які доведеться долати зловмисникові. Від складності та надійності перепони на його шляху залежить відрізок часу, необхідного на подолання кожної зони, та ймовірність того, що розташовані в кожній зоні засоби виявлення (охороні пости, охоронна сигналізація та охоронне телебачення) виявлять наявність порушника та подадуть сигнал тривоги.

Основу планування та обладнання зон безпеки об'єкта складає принцип рівноміцності меж зон безпеки. Сумарна міцність зон безпеки буде оцінюватися

найменшою з них.

Останніми роками велика увага надається створенню **систем фізичного захисту,** сполучених із системами сигналізації. Так, відома електронна система сигналізації для використання з дротовим загородженням. Система складається з електронних датчиків та мікропроцесора, який керує блоком обробки даних. Загородження довжиною до 100 м може встановлюватися на відкритій місцевості або розташовуватися на стінах, горищах та на наявних огорожах.

Фізичні засоби є першою перешкодою (бар'єром) для зловмисника при реалізації ним заходових методів доступу.

Апаратні засоби захисту

До апаратних засобів захисту інформації відносяться найрізноманітніші за принципом дії, побудовою та можливостями технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступові до джерел конфіденційної інформації.

Апаратні засоби захисту інформації - це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку і несанкціонованого доступу.

Для захисту центральних процесорів (ЦП) застосовується кодове резервування - створення додаткових бітів у форматах машинних команд (розрядів секретності) і резервних регістрів (у пристроях ЦП). Одночасно передбачаються два можливих режими роботи процесора, які відділяють допоміжні операції від операцій безпосереднього вирішення задач користувача. Для цього служить спеціальна програма переривань, яка реалізується апаратними засобами.

Одним із заходів апаратного захисту ПК та інформаційних мереж є обмеження доступу до оперативної пам'яті за допомогою встановлення меж або полів. Для цього створюються регістри контролю та регістри захисту даних. Застосовуються також додаткові біти парності - різновид методів кодового резервування.

Для позначення ступеню конфіденційності програм і даних, категорій користувачів використовуються біти, які називаються бітами конфіденційності (це два-три додаткових розряди, за допомогою яких кодуються категорії секретності користувачів, програм, даних).

Програми та дані, які завантажуються в ОЗП, потребують захисту, який гарантує їх від несанкціонованого доступу. Часто використовуються біти парності, ключі, постійна спеціальна пам'ять. При зчитуванні з ОЗП необхідно, щоб програми не могли бути знищені несанкціонованими діями користувачів або внаслідок виходу з ладу апаратури. Відмови повинні своєчасно виявлятися та усуватися, щоб запобігти виконанню спотвореної команди ЦП та втрати інформації.

Для попередження зчитування даних в ОЗП, які залишилися після обробки, застосовується спеціальна програма стирання. У цьому випадку формується команда на стирання ОЗП та вказується адреса блоку пам'яті, який повинен бути звільнений від інформації. Ця схема записує нулі або будь-яку іншу послідовність символів у всі комірки даного блоку пам'яті, забезпечуючи надійне стирання раніше завантажених даних.

Апаратні засоби захисту застосовуються й у терміналах користувачів. Для попередження витоку інформації при приєднанні незареєстрованого терміналу необхідно перед видачею запитуваних даних здійснити ідентифікацію (автоматичне

визначення коду або номера) терміналу, з якого поступив запит. У багато користувальницькому режимі цього терміналу його ідентифікації недостатньо. Необхідно здійснити автентифікацію користувача, тобто встановити його дійсність та повноваження. Це необхідно і тому, що різні користувачі, зареєстровані в системі, можуть мати доступ тільки до окремих файлів, і суворо обмежені повноваження їхнього використання.

Для ідентифікації терміналу найчастіше застосовується генератор коду, включений до апаратури терміналу, а для автентифікації користувача - такі апаратні засоби як ключі, персональні кодові картки, персональний ідентифікатор, пристрої розпізнавання голосу користувача або форми його пальців. Проте найбільш розповсюдженими засобами автентифікації є паролі, перевірені не апаратними, а програмними засобами впізнавання.

Апаратні засоби захисту інформації - це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку і несанкціонованого доступу.

Програмний захист інформації - це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції захисту інформації.

Виділяють наступні напрями використання програм для забезпечення безпеки конфіденційної інформації:

- захист інформації від несанкціонованого доступу;
- захист інформації від копіювання;
- захист програм від вірусів;
- захист інформації від вірусів;
- програмний захист каналів зв'язку.

За кожним із вказаних напрямів існує достатня кількість якісних, розроблених професіональними організаціями програмних продуктів, представлених на інформаційному ринку.

Програмні засоби захисту мають наступні різновиди спеціальних програм:

- ідентифікації технічних засобів, файлів та автентифікації користувачів;
- реєстрації та контролю роботи технічних засобів та користувачів;
- обслуговування режимів обробки інформації з обмеженим доступом;
- захисту операційних систем ПК та прикладних програм користувачів;
- знищення інформації у запам'ятовуючих пристроях після використання;
- сигналізації порушень використання ресурсів;
- допоміжні програми захисту різноманітного призначення.

Ідентифікація технічних засобів і файлів, яка здійснюється програмно, реалізується на основі аналізу реєстраційних номерів різних компонентів та об'єктів інформаційної системи та співставлення їх із значеннями адрес та паролів, що зберігаються в запам'ятовуючому пристрої системи управління.

Для забезпечення надійності захисту за допомогою паролів робота системи захисту зорганізується таким чином, щоб імовірність розкриття секретного пароля та встановлення відповідності тому чи іншому ідентифікатору файлу або термінала була як можна меншою. Для цього потрібно періодично змінювати пароль, а число символів у ньому встановлювати достатньо великим.

Ефективним способом ідентифікації елементів з адресами та автентифікації

користувачів є алгоритм "запит-відповідь", відповідно до якого система захисту видає користувачеві запит на пароль, після чого він повинен дати на нього певну відповідь. Оскільки моменти введення запиту та відповіді на нього непередбачені, це ускладнює процес відгадування пароля, що забезпечує високу надійність захисту.

Одержання дозволу на доступ до тих чи інших ресурсів можна здійснити не тільки на основі використання секретного пароля та наступних процедур автентифікації та ідентифікації. Це можна зробити більш детальним способом, який враховує різні особливості режимів роботи користувачів, їхні повноваження, категорії даних і ресурсів, що запитуються. Цей спосіб реалізується спеціальними програмами, які аналізують відповідні характеристики користувачів, зміст завдань, параметри технічних і програмних засобів, пристроїв пам'яті і т.ін.

Конкретні дані запиту, які поступають у систему, порівнюються в процесі роботи програми захисту з даними, які занесені в реєстраційні секретні таблиці (матриці). Ці таблиці, а також програми для їхнього формування та обробки зберігаються в зашифрованому вигляді та знаходяться під особливим контролем адміністратора безпеки інформаційної мережі.

Для розмежування доступу окремих користувачів до певної інформації застосовуються індивідуальні заходи секретності цих файлів та особливий контроль доступу до них користувачів. Гриф секретності може формуватися у вигляді кодових слів, що складаються з трьох розрядів які зберігаються у файлі або в спеціальній таблиці. У цій же таблиці записується ідентифікатор користувача, який створив цей файл, ідентифікатори терміналів, з яких може здійснюватися доступ до даного файлу, а також їхні права на користування файлом (зчитування, редагування, стирання, оновлення, виконання і т.ін.). Важливо не допустити взаємовплив користувачів у процесі звернення до файлів. Якщо, наприклад, один запис має право редагувати декілька користувачів, то кожному з них необхідно зберегти саме його варіант редакції (робиться декілька копій запису з метою можливого аналізу та встановлення повноважень).

Криптографічні засоби захисту

Криптографія (від грец. - "секретний, прихований" і - "пишу, креслю, малюю") - спосіб тайнопису, заснований на використанні шифру, де під шифром звичайно розуміють сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка знаходиться у повідомленні.

Криптографія включає декілька розділів сучасної математики, а також спеціальні галузі фізики, теорії інформації та зв'язку і деяких інших суміжних дисциплін.

Як наука про шифри, криптографія довгий час була засекречена, оскільки застосовувалася, в основному, для захисту державних і воєнних секретів. Проте, на теперішній час методи та засоби криптографії використовуються для забезпечення інформаційної безпеки не тільки держави, але й приватних осіб та організацій. Справа тут зовсім не обов'язково в секретах. Дуже багато різноманітних відомостей циркулює по всьому світу в цифровому вигляді. І над цими відомостями буквально "висять" загрози несанкціонованого ознайомлення, нагромадження, підміни, фальсифікації і т.ін. Найбільш надійні методи захисту від таких загроз дає саме криптографія.

Для криптографічного перетворення інформації використовуються різноманітні шифрувальні засоби - такі як засоби шифрування документів, засоби шифрування мови, засоби шифрування телеграфних повідомлень та передачі даних.

Вихідна інформація, яка передається каналами зв'язку, може являти собою мову, дані, відеосигнали, називається незашифрованим повідомленням.

У пристрої шифрування повідомлення шифрується і передається незахищеним каналом зв'язку. На приймальній стороні повідомлення дешифрується для відновлення вихідного повідомлення.

Параметр, який може застосовуватися для добування окремого повідомлення називається **ключем.**

У сучасній криптографії розглядаються два типи *криптографічних алгоритмів* (ключів). Це класичні криптографічні алгоритми, засновані на використанні секретних ключів та нові криптографічні алгоритми з відкритими ключами, засновані на використанні двох типів ключів: секретного (закритого) та відкритого.

У *криптографії з відкритими ключами* є, як правило, два ключі, один з яких неможливо визначити з іншого. Якщо ключ розшифровування обчислювальними методами неможливо одержати з ключа зашифровування, то секретність інформації, зашифрованої за допомогою несекретного (відкритого) ключа, буде забезпечена. Проте цей ключ повинен бути захищеним від підміни або модифікації. Ключ розшифровування також повинен бути секретним і захищеним від підміни або модифікації.

Якщо, навпаки, обчислювальними методами неможливо одержати ключ зашифровування з ключа розшифровування, то ключ розшифровування може бути не секретним.

Розділення функцій шифрування та розшифровування на основі розділення на дві частини додаткової інформації, необхідної для виконання операцій, є тією цінною ідеєю, яка лежить в основі криптографії з відкритим ключем.

Найбільш розповсюдженим способом шифрування мовного сигналу є аналогове скремблювання та цифрове шифрування.

Аналогове скремблювання - це перетворення аналогового сигналу з будь-якими статистичними властивостями в сигнал, що змінюється за випадковим або псевдовипадковим законом. При аналоговому скремблюванні характеристики вхідного мовного повідомлення змінюються таким чином, що перетворене повідомлення стає неприйнятим для слухової системи людини, але займає ту ж саму смугу частот. Це дозволяє передавати скрембльовані сигнали звичайними телефонними каналами зв'язку.

Останнім часом знайшли широке розповсюдження системи шифрування, у яких застосовується *цифрове шифрування мовної інформації*, яка представлена у цифровій формі.

Для передавання мови в цифровій формі стандартними телефонними каналами різко скорочують смугу мовного сигналу за допомогою пристроїв, які називають *вокодерами.*

Шифрування мовної інформації у цифровій формі здійснюється відомими методами (заміною, перестановками, аналітичними перетвореннями, гамуванням і т.ін.) або за допомогою стандартних алгоритмів криптографічного перетворення. Перевагою цифрового шифрування є висока надійність закриття мовної інформації,

оскільки перехоплений сигнал являє собою випадкову цифрову послідовність. Недоліком є необхідність використання модемів, нестійка робота пристроїв шифрування в каналах із великим загасанням сигналу та з високим рівнем завад.

Апаратні, програмні, апаратно-програмні та криптографічні засоби реалізують ті чи інші послуги інформаційної безпеки різноманітними механізмами захисту, які забезпечують дотримання конфіденційності, цілісності, доступності та повноти інформації.

ЛЕКЦІЯ 5. **Захист інформаційних систем**

1. Джерела конфіденційної інформації
2. Інформаційна система як об’єкт захисту інформації
3. Рівні захисту інформаційних систем
4. Аналіз вразливостей корпоративних інформаційних систем
5. Основні принципи захисту інформації

5.1 Джерела конфіденційної інформації

Джерело інформації - це матеріальний об'єкт, що володіє певними відомостями (інформацією), що представляють конкретний інтерес для сторонніх осіб.

В загальному плані джерелами конфіденційної інформації можна вважати наступні категорії:

1. Люди (співробітники, обслуговуючий персонал, продавці, клієнти та ін.).
2. Документи будь-якого призначення.
3. Публікації: доповіді, статті, інтерв'ю, проспекти, книги та ін.
4. Технічні носії інформації й документів.
5. Технічні засоби обробки інформації.
6. Продукція, що випускається.
7. Виробничі й промислові відходи.

Люди, в якості джерел конфіденційної інформації займають особливе місце, як активні елементи, здатні виступати не тільки власниками конфіденційної інформації, але й суб'єктами зловмисних дій. Люди є і власниками і розповсюджувачами інформації в рамках своїх функціональних обов'язків. Крім того, що люди володіють важливою інформацією, вони ще здатні її аналізувати, узагальнювати, робити відповідні висновки, а також, за певних умов, приховувати, красти, продавати та виконувати інші кримінальні дії, аж до вступу в злочинні зв'язки зі зловмисниками.

Документи. Документи - це найпоширеніша форма обміну інформацією, її нагромадження та зберігання. Під документом розуміють матеріальний носій інформації (папір, кіно- і фотоплівка, магнітна стрічка й т.п.) із зафіксованої на ньому інформацією, призначеної для її використання в часі й просторі. Документ має досить різноманітне функціональне призначення. Він може бути представлений не тільки різним змістом, але й різними фізичними формами.

По спрямованості розрізняють організаційно-розпорядницькі, планові, статистичні, бухгалтерські й науково-технічні документи, що містять, по суті, всю масу відомостей про склад, стан і діяльність будь-якої організаційної структури від державного до індивідуального рівня, про будь-який виріб, товар, задум, розробку.

Публікації. Публікації - це інформаційні носії у вигляді різноманітних видань, вони діляться на первинні і вторинні. До первинних відносять книги, статті, періодичні видання, збірники, науково-технічні звіти, дисертації, рекламні проспекти, доповіді та ін. До вторинних - інформаційні карти, реферативні журнали, експрес-інформацію, огляди, бібліографічні покажчики, каталоги та ін.

Технічні носії. Інформація може бути фіксованою та нефіксованою. Фіксована інформація - це відомості, закріплені на якому-небудь фізичному носії, а нефіксована - це знання, якими володіють вчені, фахівці, працівники, які так чи інакше беруть участь у виробництві та здатні передавати ці знання іншим. Фіксована інформація різниться залежно від виду носія, на якому вона перебуває. До технічних носіїв інформації відносяться паперові носії, кіно- і фотоматеріали (мікро- і кінофільми), магнітні носії (дискети, жорсткі диски, стримери), відеозапис, інформація на екранах ПЕОМ, на табло колективного користування, на екранах промислових телевізійних установок і інших засобів.

Технічні засоби обробки інформації. Технічні засоби як джерела конфіденційної інформації є досить широкою і ємною в інформаційному плані групою джерел. По специфіці призначення й виконання їх можна розділити на дві великі групи:

- технічні засоби забезпечення виробничої і трудової діяльності;
- технічні засоби автоматизованої обробки інформації.

До групи засобів забезпечення виробничої і трудової діяльності входять всілякі технічні засоби, такі, наприклад, як телефонні апарати й телефонний зв'язок; телеграфний, фототелеграфний і факсимільний зв'язок; системи радіозв'язку (автономні, територіальні, релейні, супутникові й ін.); телевізійні (у тому числі і засоби промислового телебачення); радіоприймачі та радіотрансляційні системи; системи гучномовного зв'язку, підсилювальні системи різного призначення; засоби магнітного та відеозапису; засоби неполіграфічного розмноження документів (друкарські машинки, ксерокопіювальні апарати, факси) та інші засоби і системи. Всі ці засоби можуть бути джерелами перетворення акустичних сигналів, що містять комерційні секрети, в електричні й електромагнітні поля, здатні утворити електромагнітні канали витоку охоронюваних відомостей.

Особливу групу технічних засобів становлять автоматизовані системи обробки інформації (АСОІ). Привабливість ПЕОМ і інформаційних систем як джерел конфіденційної інформації обумовлена рядом об'єктивних особливостей, до числа яких відносяться:

- різке розширення сфери застосування інформаційної й обчислювальної

техніки (ПЕОМ, локальні й розподілені інформаційні мережі національного й міжнародного масштабу);
- збільшення обсягів оброблюваної й збереженої інформації в локальних і розподілених банках даних;
- збільшення числа користувачів ресурсами ПЕОМ та мереж: багатокористувальницький режим вилученого доступу до баз даних.

Привабливість полягає ще і в тому, що АСОІ містить досить значні асортименти інформації. У її базах даних є вся інформація про конкретне підприємство від досьє на співробітників до конкретної продукції, її характеристиках, вартості та інші відомості.

Продукція. Продукти праці виступають джерелами інформації, за якою досить активно полюють конкуренти. Особливу увагу звертають конкуренти на нову продукцію, що перебуває на стадії підготовки до виробництва. Виробництво будь-якої продукції визначається етапами «життєвого циклу»: ідеєю, макетом, дослідним зразком, випробуваннями, серійним виробництвом, експлуатацією, модернізацією та зняттям з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що проявляється різними фізичними ефектами, які у вигляді характеристик (демаскуючих ознак) можуть розкрити охоронювані відомості про вироблений товар.

Промислові та виробничі відходи. Відходи виробництва, так званий непридатний матеріал, можуть багато чого розповісти про використовувані матеріали, їх склад, особливості виробництва, технології. До них можливий доступ через смітники, місця збору металобрухту, ящики відходів дослідницьких лабораторій, сміттєві кошики кабінетів. Не менш серйозними джерелами конфіденційної інформації є промислові відходи: стружка, обрізки, зіпсовані заготівлі, поламані комплектуючі і т.д. Аналіз відходів допоможе довідатися про особливості виробництва, технології.

Як кожне окремо, так і в сукупності джерела конфіденційної інформації містять досить повні відомості про склад, стан і напрямки діяльності підприємства.

5.2 Інформаційна система як об’єкт захисту інформації

Загалом, інформація являє собою незамінну сировину для вироблення будь-якого рішення, яку необхідно добути, переробити та поставити до закінчення терміну придатності тому, кому вона потрібна, тобто цінні відомості, що добуваються на превелику силу, повинні вчасно надійти тому, кому вони необхідні, оскільки інформація корисна тільки тоді, коли її можна використовувати для прийняття серйозних рішень. Все це визначає необхідність впровадження складних систем збору, обробки й аналізу різної інформації.

При вирішенні проблеми задоволення інформаційної потреби необхідно мати на увазі три компоненти: людину (споживача інформації), що формулює свої задачі; інформаційний фонд (інформаційний ресурс), у якому зосереджена необхідна людині інформація, і відповідний пристрій, що є посередником між споживачем і інформаційним масивом. Набір перелічених компонент і являє собою інформаційну систему.

Інформаційна система (ІС), як і будь-яка інша, має певну структуру, склад, фахівців, засоби, обладнання і порядок функціонування.

Продуктом інформаційної системи є інформація, властивості якої змінюються відповідно до заданої технології за допомогою комплексу різних технічних засобів і людей, що виконують певні технологічні операції. Відомо, що технологічні операції - це сукупність дій, спрямованих на зміну стану предмета виробництва. В інформаційній системі предметом виробництва є інформація, що на виході системи набуває потрібного користувачу вигляду та змісту.

У структуру інформаційної системи входять наступні складові:

1. Користувачі.

2. Інформаційні ресурси , документи та масиви документів в різних формах та видах (бібліотеки, архіви, фонди, бази даних, бази знань, а також інші форми організації та зберігання інформації), які містять інформацію по всім напрямкам життєдіяльності суспільства.

3. Носії інформації:

- на паперовій основі;
- звуконосії;
- фото носії;
- відео носії;
- магнітні носії;
- спеціальні технічні носії.

4. Засоби збору, зберігання та обробки інформ-традиційні технічні засоби (:телефон, радіо, звукопідсилювальні системи, поліграфія) та автоматизовані системи збору та обробки інформації.

5. Засоби передачі інформації (дротові, радіо, волоконно-оптичні)

Вихідною матеріальною основою роботи інформаційної системи виступають інформаційні ресурси. Ресурсами, як відомо, називають елементи економічного потенціалу, які перебувають у власності суспільства і які при необхідності можуть бути використані для досягнення конкретних цілей господарського й соціального розвитку.

Інформаційні ресурси можуть бути фіксованими й нефіксованими. Фіксовані інформаційні ресурси являють собою інформацію, закріплену на якому-небудь фізичному носії, а нефіксовані - знання, якими володіють люди (учені, фахівці, працівники), що беруть участь у суспільному виробництві та здатні передавати ці знання іншим учасникам виробничого процесу.

Об’єктом захисту виступає інформаційна система, предметом захисту інформації в інформаційній системі є інформація.

Для інформаційних систем як об’єктів безпеки властиві наступні характеристики: конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі.

Конфіденційність (від лат. confidential - довір’я) - це властивість не підлягати розголошенню.

Конфіденційність інформації (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність у загальному сенсі представляється як можливість доступу до

інформаційних ресурсів при їх обробці, зберіганні та передачі.

Для інформаційної системи - це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних в інформаційній системі - це властивість даних, що полягає у можливості їхнього отримання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів та ін.

Цілісність - це внутрішня єдність, зв'язаність усіх частин інформаційних ресурсів при їх обробці, зберіганні та передачі, як одного цілого в інформаційній системі. Тобто, це стан даних, або інформаційної системи, коли дані та програми використовуються встановленим чином, що забезпечує:

– стійку роботу системи;

– автоматичне відновлення у випадку виявлення системою потенційної помилки;

– автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи.

Цілісність даних в інформаційній системі - це стан, при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Семантична цілісність даних - це стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації - це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом.

Цілісність бази даних - це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємного не протиріччя. Підтримка цілісності бази даних містить перевірку цілісності і відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

Цілісність системи - це властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Захищена інформаційна система - інформаційна система, яка для певних умов експлуатації забезпечує безпеку (конфіденційність, цілісність) інформації, що функціонує в системі, та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

5.3 Рівні захисту інформаційних систем

Побудова надійного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз безпеки системи. Цей аналіз повинен складатися з таких етапів:

– виявлення характеру інформації, яка зберігається в системі;

– оцінки цінності інформації, яка зберігається в системі;

– побудови моделі зловмисника;

– визначення та класифікації загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т.д.);

– визначення затрат часу і матеріальних ресурсів на злам системи, припустимих для зловмисників;

– оцінки припустимих витрат часу, засобів і ресурсів системи на організацію її захисту.

Проблеми інформаційної безпеки вирішуються, як правило, з допомогою створення спеціалізованих систем захисту інформації, які повинні забезпечувати безпеку інформаційної системи від несанкціонованого доступу до інформаційних ресурсів. Система захисту інформації є інструментом адміністраторів інформаційної безпеки, які виконують функції із забезпечення захисту інформаційної системи і контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

– реєстрація і облік користувачів, носіїв інформації, інформаційних масивів;

– забезпечення цілісності системного та прикладного програмного забезпечення та інформації яка оброблюється;

– захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту;

– створення захищеного електронного документообігу з використанням сертифікованих засобів криптографічні перетворення і електронного цифрового підпису;

– централізоване управління системою захисту інформації;

– управління доступом;

– забезпечення ефективного антивірусного захисту, тощо.

Комплекс вимог, які висуваються до системи безпеки, передбачає функціональне навантаження на кожний з наведених на рис. 5.1. рівнів.

Організація захисту на фізичному рівні повинна зменшити можливість несанкціонованих дій сторонніх осіб і персоналу підприємства, а також понизити вплив техногенних джерел.

Захист на технологічному рівні (програмний продукт і технічні засоби обробки інформації). Система захисту на цьому рівні повинна бути автономною, але забезпечувати реалізацію єдиної політики безпеки і будуватись на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

Рис. 5.1. Рівні захисту інформаційної системи

На локальному рівні зорганізується розподілення інформаційних ресурсів ІС на сегменти за рівнями конфіденційності по територіальному і функціональному принципах, а також виділяється в окремий сегмент засоби обробки конфіденційної інформації. Підвищенню рівня захищеності сприяє обмеження і мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і інформаційної системи в цілому, організація захищеного обміну інформацією між сегментами.

На мережевому рівні зорганізується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється надійна оболонка фізичного захисту периметра розташування ІС в цілому. Система захисту на цьому рівні повинна будуватись з урахуванням реалізації захисту на попередніх рівнях.

На рівні користувача повинно бути забезпечено допуск тільки авторизованих абонентів до роботи в інформаційний системі, створено захисну оболонку навколо її елементів, а також організовано індивідуальне захищене середовище діяльності кожного користувача.

Залежно від призначення і характеру задач з обробки інформації можна виділити три основні види експлуатації інформаційних систем, що мають принципове значення для складу посадовців і характеру доступу до інформації з:

– **закритим доступом** - організація - споживач використовує інформаційну систему повністю в своїх інтересах, при цьому обслуговуючий персонал, включаючи технічний і оперативний склад, є співробітниками даної організації;

– **обмеженим доступом** - організація - споживач обчислювальної системи поєднує свої інтереси з інтересами інших організацій і приватних осіб;

– **відкритим доступом** - організація - споживач обчислювальної мережі надає послуги населенню.

Назва «Система з відкритим доступом» умовна в тому значенні, що будь-яка людина може скористатися послугами даної системи. Насправді ж кожна інформаційна система має і внутрішню частину, яка стосується обробки її власної інформації, яка може бути закритою для сторонніх осіб.

Усі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в системі. Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації.

Дослідження і аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою. Попередження зазначених наслідків в інформаційній системі є основною метою створення системи безпеки інформації, розроблення та вдосконалення існуючих методів захисту інформації.

Для вирішення поставленої задачі доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в ІС.

Можна виділити такі основні класи загроз безпеці, які спрямовані проти інформаційних ресурсів:

– загрози конфіденційності даних і програм;

– загрози цілісності даних, програм, апаратури;

– загрози доступності даних;

– загрози відмови від виконання трансакцій.

Оцінка вразливості інформаційної системи і побудова моделі впливів припускають вивчення всіх варіантів реалізації перерахованих вище загроз і виявлення наслідків, до яких вони призводять.

5.4 Аналіз вразливостей корпоративних інформаційних систем

Корпоративна інформаційна система (КІС) - це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві (в корпорації) і постачає інформацію для прийняття управлінських рішень. У ній реалізована управлінська ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології. В загальному випадку КІС - це система з можливістю масштабування, призначена для комплексної автоматизації всіх видів господарської діяльності великих і середніх підприємств, в тому числі корпорацій, що складаються з групи компаній, які потребують єдиного управління. Об'єднує систему управління персоналом, матеріальними, фінансовими та іншими ресурсами компанії, використовується для підтримки планування і управління компанією, для підтримки прийняття управлінських рішень її керівниками. Під КІС можна розуміти управлінську ідеологію, яка об'єднує бізнес-стратегію та інформаційні технології.

До основних принципів побудови КІС належать:

- інтелектуальність (управління організацією - реєстрація та накопичення інформації);
- інтегрованість (наскрізне проходження документів через різні служби);
- модульність (можливість поетапного впровадження системи);
- доступність;
- відкритість (можливість взаємодіяти з іншими програмами);
- адаптивність (потужність механізму налаштувань).

Основні вимоги КІС:

- використання архітектури клієнт-сервер з можливістю застосування промислових СУБД;

– забезпечення безпеки методами контролю і розмежування доступу до інформаційних ресурсів;
– підтримку розподіленої обробки інформації;
– модульний принцип побудови з оперативно-незалежних функціональних блоків з розширенням за рахунок відкритих стандартів (API, COM і інші).

Корпоративні інформаційні системи діляться на наступні класи:
– ERP (Enterprise Resource Planning System);
– CRM (Customer Relationship Management System);
– MES (Manufacturing Execution System);
– WMS (Warehouse Management System);
– EAM (Enterprise Asset Management);
– HRM (Human Resource Management);
– СЕД (Системи електронного документообігу).

Підходи побудови КІС:
– орієнтація на споживача;
– процесний підхід;
– збалансована система показників (відношення клієнта до компанії, ступінь його задоволеності, інноваційний потенціал компанії і співробітників, якість бізнес-процесів та ін.);
– комплексний підхід до управління;
– системний підхід;
– адаптивне управління (вибір оптимального способу досягнення мети, це спосіб управління, при якому зберігаються незмінними цільові показники).

Головними особливостями сучасного підходу до побудови корпоративної інформаційної системи підприємства є:
– всебічний аналіз бізнес-процесів, на основі якого проводиться розробка проекту інформаційної системи і обґрунтування закладених в ньому рішень;
– використання широкої палітри сучасних методологій та інструментальних засобів моделювання та проектування систем;
– підтримка міжкорпоративного бізнесу;
– детальне опрацювання та узгодження з замовником всіх етапів розробки проекту, контрольних точок, необхідних ресурсів.

Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи. Для більшості корпорацій з розподіленою інфраструктурою процес безперервного забезпечення комплексного захисту інформаційних активів стає непростим завданням через високу складності архітектури і великого числа взаємозв'язків всередині окремих підсистем. За результатами аналітики в 2019 році найбільш поширені уразливості на мережевому периметрі корпоративних інформаційних систем розподілені наступним чином:

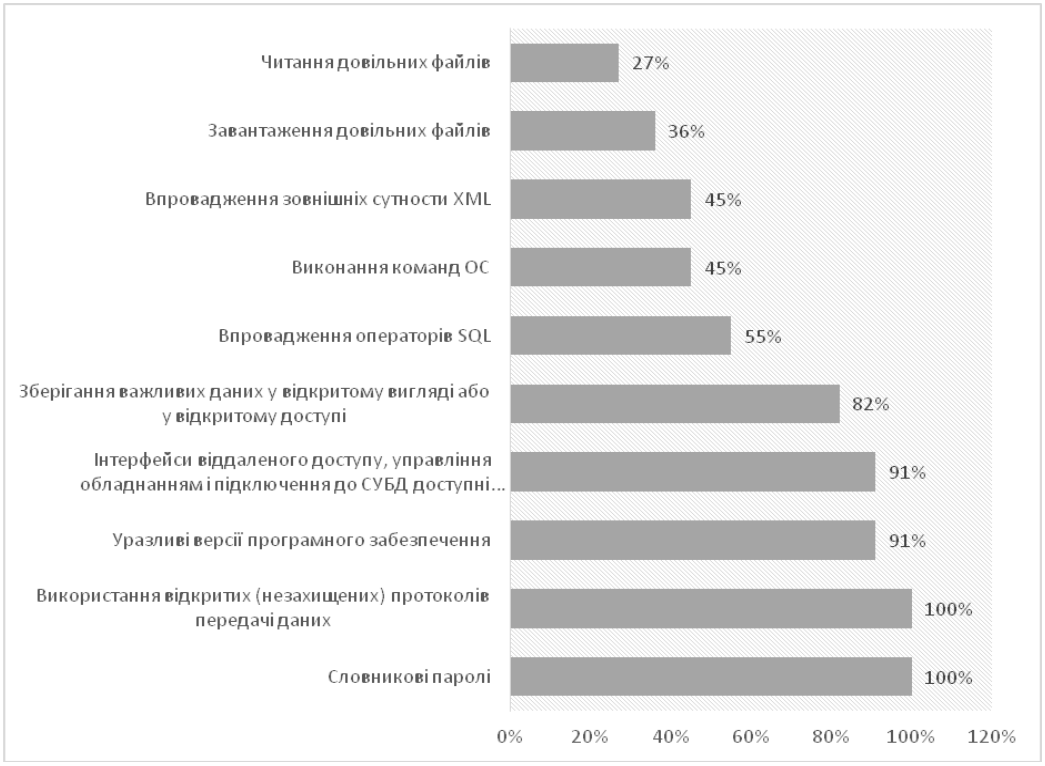

Рис. 5.2. Найбільш поширені уразливості на мережевому периметрі (частка систем)*

**Джерело за даними аналітики компанії Positive Technologies 2019 рік.*

Локальна обчислювальна мережа є основою функціонування будь-якої КІС. До найбільш поширених загроз інформаційної безпеки даного типу мереж належать:

10. Недоліки захисту службових протоколів, що призводять до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі.
11. Словникові паролі.
12. Недостатній рівень захисту привілейованих облікових записів.
13. Зберігання важливої інформації у відкритому вигляді.
14. Недоліки захисту протоколів NBNS і LLMNR.
15. Недостатньо ефективна реалізація антивірусного захисту.
16. Використання слабких алгоритмів шифрування при зберіганні паролів.
17. Уразливі версії програмного забезпечення.
18. Надлишкові привілеї додатків або СУБД.
19. Використання відкритих (незахищених) протоколів передачі даних.

В той же час корпоративні інформаційні системи мають свої характерні вразливості інформаційної безпеки. До них можна віднести:

1. Помилки в коді веб-додатків і відсутність оновлень безпеки.
2. Недоліки конфігурування.

За даними результатів аналітики провідних компаній, які займаються інформаційною безпекою підприємств останніми роками зберігається тенденція до підвищення загального рівня захищеності мережевого периметра корпоративних інформаційних систем. В середньому, у 27% випадків фахівцям не вдається подолати мережевий периметр і отримати доступ до ресурсів внутрішньої локальної обчислювальної мережі. Дані результати пов'язані з тим, що деякі замовники регулярно проводять тестування на проникнення і усувають виявлені вразливості. Однак важливо пам'ятати, що конфігурація мережевої інфраструктури регулярно змінюється, тому тестування на проникнення необхідно проводити на регулярній

основі. Крім того, потрібно стежити за тим, які служби доступні для підключення з мережі Інтернет. Приклади подолання периметра і отримання доступу до ресурсів локальної обчислювальної мережі:

1. Тривіальна складність подолання периметра. На периметрі мережі доступний для підключення інтерфейс налагодження JDWP. Будь-який зовнішній порушник може використовувати загальнодоступний експлойт (github.com/IOActive / jdwp-shellifier) і виконати довільні команди на сервері. Використовуючи цю вразливість і надлишкові привілеї служби, вдається отримати повний контроль над сервером і доступ до ЛВС (якщо на вузлі є доступ до інтерфейсу внутрішньої мережі).

2. Низька складність подолання периметра. На тестованому вузлі виявлено веб-додаток для управління навчанням співробітників. Шляхом реєстрації нового облікового запису без підтвердження особи вдається отримати доступ до функціональності веб-додатка і завантажити веб-інтерпретатор командного рядка (веб-шелл) на сервер, що робить можливим виконання довільних команд ОС на сервері з привілеями веб-додатка. Таким чином вдається отримати доступ до ЛОМ, у випадку, коли на вузлі є доступний інтерфейс внутрішньої мережі.

3. Середня складність подолання периметра. В ході робіт по оцінці обізнаності співробітників в питаннях інформаційної безпеки була проведена масова розсилка електронних листів від внутрішньої особи з посиланням на веб-ресурс, що містить фішингову форму для введення облікових даних. Деякі співробітники ввели облікові дані в помилкову форму аутентифікації. Отримані облікові дані можуть бути використані для несанкціонованого доступу до ресурсів системи. Для використання фішингових сценаріїв атак як мінімум необхідно зареєструвати власний домен і розробити неправдиву форму аутентифікації. Більш того, важливо зробити фішинговий ресурс максимально наближеним по дизайну сторінки до того ресурсу, яким звик користуватися співробітник. Для цього необхідно проводити додаткові розвідувальні дії, що істотно підвищує складність реалізації атаки.

Після отримання доступу до внутрішньої мережі зовнішній зловмисник має можливості для розвитку атаки і отримання повного контролю над всією IT-інфраструктурою або окремими критично важливими системами.

У більшості випадків для отримання максимальних привілей в критично важливих системах від імені внутрішнього порушника досить підібрати обліковий запис з привілеями локального адміністратора на одній з робочих станцій або на сервері ЛОМ, запустити спеціалізоване ПО і отримати у відкритому вигляді облікові записи локальних адміністраторів інших вузлів. Даний вектор атаки можна розвивати аж до отримання облікових даних адміністраторів доменів.

За результатами звітів компаній, діяльністю яких є аналіз та захист інформаційної безпеки підприємств, перше місце в рейтингу найбільш поширених уразливостей захисту внутрішніх ресурсів належить недолікам захисту протоколів мережевого і канального рівнів, що призводить до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі. Кожна досліджувана система містила різні недоліки захисту службових протоколів, таких як ARP, STP, BOOTP, CDP. У кожному з проектів, де проводився аналіз мережевого трафіку ЛОМ, було виявлено відсутність механізмів захисту від атак ARP Cache Poisoning. Даний недолік може бути використаний для прослуховування трафіку в мережі і проведення атак типу «людина посередині». В ході успішної реалізації атаки

порушник може перехоплювати конфіденційну інформацію, змінювати дані в процесі передачі і блокувати мережеву взаємодію.

На другому місці серед уразливостей внутрішніх мереж знаходиться використання словникових паролів. Третє місце - недостатній рівень захисту привілейованих облікових записів.

Таким чином, можна зробити наступні висновки: сучасні корпоративні інформаційні системи мають велику кількість уразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації. Досить низьким є рівень захищеності бездротових мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки.

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених уразливостей і недоліків, для усунення яких, як правило, досить застосувати базові принципи забезпечення інформаційної безпеки:

- використовувати сувору парольну політику;
- захищати привілейовані облікові записи;
- не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі;
- обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб;
- захищати або відключати в локальній обчислювальній мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;
- мінімізувати привілеї користувачів і служб;
- регулярно оновлювати ПЗ і встановлювати оновлення безпеки ОС;
- для своєчасного виявлення атак використовувати SIEM-системи;
- для захисту веб-додатків використовувати web application firewalls;
- проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки (при цьому важливо проводити і оцінку ефективності таких тренінгів);
- регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці.

При цьому важливо забезпечити всі ці заходи в комплексі, тільки тоді захист буде ефективним, а витрати на різні дорогі рішення виявляться виправданими.

5.5 Основні принципи захисту інформації

Захист інформації від НСД є складовою частиною загальної проблеми забезпечення захисту інформації в ІС. В загальному випадку комплекс програмно-технічних засобів та організаційних рішень по захисту інформації в ІС реалізується в рамках системи захисту інформації від НСД, яка умовно складається з таких чотирьох підсистем:

– управління доступом до ІС, до її послуг та ресурсів;
– реєстрація і облік користувачів, послуг, інформаційних ресурсів;
– криптографічного захисту;
– забезпечення цілісності інформаційних потоків, інформаційних ресурсів та

програмного забезпечення.

Закриття каналів несанкціонованого отримання інформації повинно починатися з контролю доступу користувачів до ресурсів ІС. Ця задача вирішується на основі ряду принципів:

Принцип виправданості доступу - користувач повинен мати достатню «форму допуску» для отримання інформації того рівня конфіденційності, що він вимагає, і ця інформація дійсно необхідна йому для виконання його виробничих функцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів ІС, які у відповідності з принципом виправданості доступу слід розмежовувати між користувачами.

Принцип розмежування інформаційних потоків. Для попередження порушення інформаційної безпеки, яке, наприклад, може мати місце при запису секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, які не призначені для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах зв'язку, необхідно здійснювати відповідне розмежування інформаційних потоків.

Принцип персональної відповідальності. Кожний користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту. Даний принцип передбачає, що засоби захисту інформації в ІС повинні чітко виконувати свої функції у відповідності з переліченими принципами і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так званого «монітору звернень», який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами доступу до цих даних і програм. Схематично такий монітор можна представити у вигляді, показаному на рис. 5.3.

Рис. 5.3. Структура монітору звернень

Практичне створення монітору звернень, як видно з наведеного рисунку, передбачає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації.

Найбільш розповсюджена модель отримала назву - багаторівнева модель захисту Белла Ла Падула. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На основі присвоєних кожному суб'єкту і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді і тільки тоді, коли відповідний йому рівень конфіденційності більше чи дорівнює конфіденційності іншого, а множина категорій включає множину категорій другого.

ЛЕКЦІЯ 6. **Інформаційно-комунікаційні системи та комп'ютерні мережі**

1. Інформаційно-комунікаційні системи
2. Захист інформації в комп'ютерних мережах
3. Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC
4. Задачі організації безпеки інформації та інформаційних ресурсів

6.1 Інформаційно-комунікаційні системи.

Впровадження та інтеграція інформаційно-комунікаційних систем та мереж потребує високого рівня технічних і соціальних вимог до якості інформаційних ресурсів та безпосередньо до систем передачі, обробки і відображення даних. Базовими властивостями інформаційних ресурсів є їх цілісність, конфіденційність і доступність. Випадкові, а також штучні завади, спотворюють інформаційні потоки, які надходять від джерела повідомлення до споживача, що призводить до втрати цілісності даних. Спотворення основних властивостей інформації при її передачі чи обробці, веде до неякісних процедур прийняття рішень або зовсім унеможливлює цей процес у всіх сферах діяльності розвинутого суспільства.

Базовою функцією інформаційних систем передачі даних є здійснення процесів оперативного та надійного обміну інформацією між джерелом повідомлення та його користувачем, а також у забезпеченні ефективності функціонування інформаційної системи мінімізації часу передачі інформації за умов зростання її обсягів при фіксованій вірогідності інформаційного потоку. Інформаційні системи передачі даних є базовою платформою сучасного процесу інформатизації суспільства, що активно впливає на стан національної безпеки держави.

Інформаційно-комунікаційна система (та комп'ютерна мережа, ІКСМ) - це інтегрований комплекс організаційно-технічних заходів та взаємопов'язаних і взаємоузгоджених комунікаційних, програмно-апаратних і програмних компонентів, які забезпечують достовірну передачу інформації від джерела повідомлення до споживача.

Вивчення мережі в цілому потребує знання принципів роботи та характеристик її окремих елементів: комп'ютерів, комунікаційного устаткування, операційних систем, мережних додатків і т. ін.

Багаторівневою моделлю інформаційно-комунікаційної системи називається повний інтегрований комплекс середовища та комунікаційних й програмно-апаратних засобів, що застосовується з метою достовірної передачі інформаційних потоків від джерела повідомлення до споживача.

Перший (апаратний) рівень - основа будь-якої мережі, створена стандартизованими комп'ютерними платформами й використовувана з метою автоматизованої обробки даних.

Другий рівень - комунікаційне устаткування зазначеної інформаційно-комунікаційної мережі.

Не зважаючи на те, що комп'ютери і є центральними елементами обробки даних у мережах, не менш важливу роль в організації мережі відіграють комунікаційні пристрої. Кабельні системи, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори - усі ці складові перетворилися з допоміжних компонентів мережі на основні як за впливом на характеристики

мережі, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим мультипроцесором, який потрібно конфігурувати, оптимізувати й адмініструвати. Для вивчення принципів роботи комунікаційного устаткування необхідно знання великої кількості протоколів, використовуваних як у локальних, так і у глобальних мережах.

Третій рівень - операційні системи (ОС), які створюють та забезпечують програмну платформу мережі.

Від того, які концепції управління локальними та розподіленими ресурсами покладено в основу мережної ОС, залежить ефективність роботи всієї мережі. При проектуванні мережі важливо враховувати:

– оптимальність взаємодії даної операційної системи з іншими ОС мережі;

– можливість нарощувати кількість користувачів (складність мережі);

– можливість адаптації чи інсталяції на інші типи обчислювальних платформ тощо.

Четвертий рівень - рівень мережних засобів - утворюють мережні додатки, такі як мережні бази даних, поштові системи, засоби архівації даних, системи автоматизації колективної роботи і т. ін.

Важливо уявляти діапазон можливостей, що надаються додатками для різних сфер застосування, а також знати, наскільки вони сумісні з іншими мережними додатками й операційними системами.

Мережева технологія - це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують (наприклад, мережевих адаптерів, драйверів, кабелів і роз'ємів), достатніх для побудови та функціонування інформаційно-комунікаційної (комп'ютерної) мережі.

Однією з найбільш розвинених мережевих технологій є технологія Ethernet. Протоколи, на основі яких будується мережа певної технології (у вузькому сенсі), спеціально розроблялися для спільної роботи користувачів (абонентів), тому від розробника мережі не вимагається додаткових зусиль щодо організації її взаємодії. Іноді мережні технології називають базовими, маючи на увазі те, що на їх основі будується базис будь-якої мережі.

Головний принцип, покладений в основу Ethernet, - випадковий метод доступу до середовища передачі даних та загальних інформаційних ресурсів (CSMA/CD). Як середовище може використовуватися товстий або тонкий коаксіальний кабель, вита пара, оптоволокно або радіохвилі для передачі інформаційних потоків.

Сутність випадкового методу доступу: користувач у мережі Ethernet може передавати дані по мережі тільки тоді, коли мережа вільна, тобто коли ніякий інший користувач (комп'ютер) у даний момент не обмінюється даними. Тому важливою частиною технології Ethernet є процедура визначення доступності середовища.

При об'єднанні в мережу великої кількості користувачів постає цілий комплекс технічних та інших питань. Проектування мережі передусім передбачає в тому числі розв'язання задачі про забезпечення безпеки інформації і захищеності даних.

6.2 Захист інформації в комп'ютерних мережах

Комп'ютерна мережа - система зв'язку між двома чи більше комп'ютерами. У більш широкому розумінні комп'ютерна мережа - це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і

мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило - різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали. Мережа дає можливість окремим співробітникам організації взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів; дозволяє їм одержувати доступ до даних, що зберігається на персональних комп’ютерах у видалених офісах, і встановлювати зв’язок з постачальниками. Мережеві операції регулюються набором правил і угод (званих мережевим протоколом), який визначає: типи роз’ємів і кабелів, види сигналів, формати даних, алгоритми роботи мережевих інтерфейсів, способи контролю та виправлення помилок, взаємодія прикладних процесів та ін.

До теперішнього часу розроблено значну кількість організаційних та архітектурних різновидів побудови комп’ютерних мереж. Системну їх класифікацію можна здійснити за наступними критеріями:

1) за масштабом - локальні та глобальні;

2) за способом організації - централізовані і децентралізовані;

3) по топології (конфігурації) - зіркоподібні, кільцеві, шинні, змішані.

Різновиди комп’ютерних мереж по виділених значенням перерахованих критеріїв характеризуються наступним чином:

– локальні обчислювальні мережі - мережі, вузли яких розташовуються на невеликих відстанях один від одного (в різних приміщеннях однієї і тієї ж будівлі, в різних будівлях, розташованих на одній і тій же території).

– глобальні обчислювальні мережі - вузли мережі розташовані на значних відстанях один від одного (в різних частинах великого міста, у віддалених один від одного населених пунктах (які включають у себе цегляні, панельні і дерев'яні будинки), в різних регіонах країни і навіть у різних країнах).

Централізовані локальні обчислювальні мережі - мережі, в яких передбачено головний вузол, через який здійснюються всі обміни інформацією і який здійснює управління всіма процесами взаємодії вузлів.

Децентралізовані обчислювальні мережі - мережі з відносно рівноправними вузлами, управління доступом до каналів передачі даних у цих мережах розподілено між вузлами.

На основі навіть такого швидкого розгляду можливих структур обчислювальних мереж неважко зробити висновок, що для тих об'єктів (підприємств, установ, інших організацій), в яких регулярно обробляються значні обсяги інформації, найбільш доцільною буде комбінована структура комп’ютерних обчислювальних мереж.

Мережева взаємодія

Дане питання розглянемо на прикладі найбільш поширеної і визнаної еталонної моделі взаємодії відкритих систем ISO / OSI (BOC) [1].

В основу еталонної моделі покладена ідея декомпозиції процесу функціонування відкритих систем на рівнях, причому розбиття на рівні проводиться таким чином, щоб згрупувати в рамках кожного з них функціонально найбільш близькі компоненти. Крім того, потрібно, щоб взаємодія між суміжними рівнями була мінімальною, число рівнів порівняно невеликим, а зміни, вироблені в рамках

одного рівня, не вимагали б перебудови суміжних.

Окремий рівень, таким чином, являє собою логічно і функціонально замкнуту підсистему, що сполучається з іншими рівнями за допомогою спеціально визначеного інтерфейсу. В рамках моделі ISO/OSI кожен конкретний рівень може взаємодіяти тільки із сусідніми. Сукупність правил (процедур) взаємодії об'єктів однойменних рівнів називається протоколом.

Еталонна модель містить сім рівнів (знизу вгору):

1. Фізичний.
2. Канальний (або передачі даних).
3. Мережевий.
4. Транспортний.
5. Сеансовий.
6. Представницький.
7. Рівень додатків.

Кожен рівень передавальної станції в цій ієрархічній структурі взаємодіє з відповідним рівнем приймаючої станції за допомогою нижчих рівнів. При цьому кожна пара рівнів за допомогою службової інформації повідомлень встановлює між собою логічне з'єднання, забезпечуючи тим самим логічний канал зв'язку відповідного рівня. За допомогою такого логічного каналу кожна пара верхніх рівнів може забезпечувати між собою взаємодію, абстрагуючись від особливостей нижніх. Іншими словами, кожен рівень реалізує строго певний набір функцій, який може використовуватися верхніми рівнями незалежно від деталей реалізації цих функцій (див. Табл.)

Таблиця. Семирівнева модель протоколів мережевого обміну ISO

№ рівня	Найменування рівня	Зміст
7	Рівень додатків	Надання послуг на рівні кінцевого користувача
6	Рівень представлення даних	Інтерпретація та стиск даних
5	Рівень сеансів	Аутентифікація та перевірка повноважень
4	Транспортний рівень	Забезпечення коректної передачі даних
3	Мережевий рівень	Маршрутизація та ведення обліку
2	Канальний рівень	Передача та прийом пакетів, визначення апаратних адрес
1	Фізичний рівень	Кабель або фізичний носій інформації

Розглянемо докладніше функціональне призначення кожного рівня.

Фізичний рівень. Фізичний рівень забезпечує електричні, функціональні та процедурні засоби встановлення, підтримки і роз'єднання фізичного з'єднання. Реально він представлений апаратурою генерації та управління електричними сигналами і каналом передачі даних. На цьому дані представляються у вигляді послідовності бітів або аналогового електричного сигналу. Завданням фізичного рівня є передача послідовності бітів з буфера відправника в буфер одержувача.

Канальний рівень. Протоколи канального рівня (або протоколи управління

ланкою передачі даних) займають особливе місце в ієрархії рівнів: вони служать сполучною ланкою між реальним каналом, що забезпечує безпомилкову передачу даних. Цей рівень використовується для організації зв'язку між двома станціями за допомогою наявного (зазвичай ненадійного) каналу зв'язку. При цьому станції можуть бути пов'язані декількома каналами.

Протокол канального рівня повинен забезпечити наступне:

– незалежність протоколів вищих рівнів від використовуваного середовища передачі даних;

– кодонезалежність переданих даних;

– вибір якості обслуговування при передачі даних.

На цьому рівні дані представляються кадром, який містить інформаційне поле, а також заголовок і доповнення (трейлер), що привласнюються протоколом. Заголовок містить службову інформацію, використовувану протоколом канального рівня приймаючої станції і служить для ідентифікації повідомлення, правильного прийому кадрів, відновлення і повторної передачі у разі помилок і т. д. Доповнення містить перевірочне поле, що служить для корекції та виправлення помилок, внесених каналом. Завдання протоколу канального рівня - складання кадрів, правильна передача і прийом послідовності кадрів, контроль послідовності кадрів, виявлення та виправлення помилок в інформаційному полі (якщо це необхідно).

Мережевий рівень. Мережевий рівень надає транспортному рівню набір послуг, головними з яких є наскрізна передача блоків даних між передавальною і приймальною станціями (тобто, виконання функцій маршрутизації та ретрансляції) і глобальне адресування користувачів. Іншими словами, знаходження одержувача за вказаною адресою, вибір оптимального (в умовах даної мережі) маршруту та доставка блоку повідомлення за вказаною адресою.

Таким чином, на кордоні мережевого і транспортного рівнів забезпечується незалежність процесу передачі даних від використовуваних середовищ за винятком якості обслуговування. Під якістю обслуговування розуміється набір параметрів, що забезпечують функціонування мережевої служби, що відображає робочі (транзитна затримка, коефіцієнт невиявлених помилок та ін.) Та інші характеристики (захист від НСД, вартість, пріоритет та ін.). Система адрес, використовувана на мережевому рівні, повинна мати ієрархічну структуру і забезпечувати наступні властивості: глобальну однозначність, маршрутну незалежність і незалежність від рівня послуг.

На мережевому рівні дані представляються у вигляді пакету, який містить інформаційне поле і заголовок, який присвоюється протоколом. Заголовок пакета містить керуючу інформацію, яка вказує адресу відправника, можливо, маршрут і параметри передачі пакета (пріоритет, номер пакета в повідомленні, параметри безпеки, максимум ретрансляції та ін.). Розрізняють такі види мережевої взаємодії:

– з встановленням з'єднання - між відправником та одержувачем спочатку за допомогою службових пакетів організовується логічний канал (відправник - відправляє пакет, одержувач - чекає отримання пакету плюс взаємне повідомлення про помилки), який роз'єднується після закінчення повідомлення або у разі невиправної помилки. Такий спосіб використовується протоколом X.25;

– без встановлення з'єднання (дейтаграмний режим) - обмін інформацією здійснюється за допомогою дейтаграм (різновид пакетів), незалежних один від одного, які приймаються також незалежно один від одного і збираються в

повідомлення на приймальній станції. Такий спосіб використовується в архітектурі протоколів DARPA.

Транспортний рівень. Транспортний рівень призначений наскрізної передачі даних через мережу між кінцевими користувачами - абонентами мережі. Протоколи транспортного рівня функціонують тільки між кінцевими системами.

Основними функціями протоколів транспортного рівня є розбивка повідомлень або фрагментів повідомлень на пакети, передача пакетів через мережу і збір пакетів. Вони також виконують такі функції: відображення транспортного адреси в мережі, мультиплексування і розщеплення транспортних сполучень, міжкінцеве управління потоком і виправлення помилок. Набір процедур протоколу транспортного рівня залежить як від вимог протоколів верхнього рівня, так і від характеристик мережевого рівня.

Найбільш відомим протоколом транспортного рівня є TCP (Transmission Control Protocol), використовуваний в архітектурі протоколів DARPA і прийнятий в якості стандарту. Він використовується в якості високонадійного протоколу взаємодії між комп'ютерами в мережі з комутацією пакетів.

Протоколи верхніх рівнів. До протоколів верхніх рівнів відносяться протоколи **сеансового, представницького і прикладного рівнів**. Вони спільно виконують одну задачу - забезпечення сеансу обміну інформацією між двома прикладними процесами, причому інформація повинна бути представлена в тому вигляді, який зрозумілий обом процесам. Тому зазвичай ці три рівня розглядають спільно. Під прикладним процесом розуміється елемент кінцевої системи, який бере участь у виконанні одного або декількох завдань з обробки інформації. Зв'язок між ними здійснюється за допомогою прикладних об'єктів - елементів прикладних процесів, що беруть участь в обміні інформацією. При цьому протоколи верхніх рівнів не враховують особливості конфігурації мережі, каналів і засобів передачі інформації.

Протоколи представницького рівня надають послуги за погодженням синтаксису передачі (правил, які задають подання даних при їх передачі) і конкретним уявленням даних в прикладній системі. Іншими словами, на представницькому рівні здійснюється синтаксичне перетворення даних від виду, використовуваного на прикладному рівні, до виду, використовуваному на інших рівнях (і навпаки).

Прикладний рівень, будучи самим верхнім у еталонної моделі, забезпечує доступ прикладних процесів до середи взаємодії відкритих систем. Основним завданням протоколів прикладного рівня є інтерпретація даних, отриманих з нижніх рівнів, і виконання відповідних дій у кінцевій системі в рамках прикладного процесу. Зокрема, ці дії можуть полягати в передачі управління певним службам операційної системи разом з відповідними параметрами.

Крім того, прикладний рівень можуть надавати послуги з ідентифікації і аутентифікації партнерів, встановленню повноважень для передачі даних, перевірці параметрів безпеки, управлінню діалогом та ін.

Для мереж передачі даних реальну небезпеку представляють наступні **загрози.**

1. Прослуховування каналів, тобто запис і подальший аналіз всього потоку повідомлень. Прослуховування в більшості випадків не помічається легальними учасниками інформаційного обміну.

2. Умисне знищення або спотворення (фальсифікація) повідомлень в мережі, а

також включення в потік помилкових повідомлень. Неправдиві повідомлення можуть бути сприйняті одержувачем як справжні.

3. Присвоєння зловмисником своєму вузлу або ретранслятору чужого ідентифікатора, що дає можливість отримувати або відправляти повідомлення від чужого імені.

4. Навмисний розрив лінії зв'язку, що призводить до повного припинення доставки всіх (або тільки, обраних зловмисником) повідомлень.

5. Впровадження мережевих вірусів. Передача по мережі тіла вірусу з його подальшою активізацією користувачем віддаленого або локального вузла.

Відповідно до цього специфічні **завдання захисту в мережах передачі даних** полягають у наступному.

1. Аутентифікація однорівневих об'єктів, що полягає у підтвердженні справжності одного або декількох взаємодіючих об'єктів при обміні інформацією між ними.

2. Контроль доступу та захист від несанкціонованого використання ресурсів мережі.

3. Маскування даних, що циркулюють в мережі.

4. Контроль і відновлення цілісності всіх даних, що знаходяться в мережі.

5. Арбітражне забезпечення або захист від можливих відмов від фактів відправки, прийому або змісту відправлених або прийнятих даних.

Таким чином, стосовно до різних рівнів семирівневого протоколу передачі даних **завдання захисту інформації в мережі** можуть бути конкретизовані наступним чином.

1. Фізичний рівень - контроль електромагнітних випромінювань ліній зв'язку та пристроїв, підтримка комутаційного обладнання в робочому стані. Захист на даному рівні забезпечується за допомогою екрануючих пристроїв, генераторів перешкод, засобів фізичного захисту передавального середовища.

2. Канальний рівень - збільшення надійності захисту (при необхідності) за допомогою шифрування переданих по каналу даних. У цьому випадку шифруються всі передані дані, включаючи службову інформацію.

3. Мережевий рівень - найбільш вразливий рівень з точки зору захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком.

Крім того, протоколами мережевого рівня пакети обробляються на всіх маршрутизаторах, шлюзах та інших проміжних вузлах. Майже всі специфічні мережеві порушення здійснюються з використанням протоколів даного рівня (читання, модифікація, знищення, дублювання, переорієнтація окремих повідомлень або потоку в цілому, маскування під інший вузол і ін.). Захист від таких загроз здійснюється протоколами мережевого і транспортного рівнів і за допомогою засобів криптографічного захисту. На даному рівні може бути реалізована вибіркова маршрутизація.

4. Транспортний рівень - здійснює контроль за функціями мережевого рівня на приймальному і передавальному вузлах (на проміжних вузлах протокол транспортного рівня не функціонує). Механізми транспортного рівня перевіряють цілісність окремих пакетів даних, послідовності пакетів, пройдений маршрут, час відправлення і доставки, ідентифікацію та аутентифікацію відправника і одержувача

та інші функції. Всі активні загрози стають видимими на даному рівні.

Гарантом цілісності переданих даних є криптозахист як самих даних, так і службової інформації. Ніхто, крім тих, що мають секретний ключ одержувача і / або відправника, не може прочитати або змінити інформацію таким чином, щоб зміна залишилася непоміченою.

Аналіз трафіку забезпечується передачею повідомлень, що не містять інформацію, які, однак, виглядають як реальні повідомлення. Регулюючи інтенсивність цих повідомлень в залежності від обсягу переданої інформації, можна постійно домагатися рівномірного трафіку. Проте всі ці заходи не можуть захистити від загрози знищення, переорієнтації або затримки повідомлення. Єдиним захистом від таких порушень може бути паралельна доставка дублікатів повідомлення по інших шляхах.

5. Протоколи верхніх рівнів забезпечують контроль взаємодії прийнятої або переданої інформації з локальною системою. Протоколи сеансового і представницького рівня функцій захисту не виконують. У функції захисту протоколу прикладного рівня входить управління доступом до певних наборів даних, ідентифікація і аутентифікація певних користувачів, а також інші функції, які визначаються конкретним протоколом. Більш складними ці функції є у разі реалізації повноважної політики безпеки в мережі.

6.3 Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC

Наприкінці 90-х рр. Британський Інститут Стандартів (BSI) розробив національний стандарт щодо управління інформаційною безпекою, який потім одержав назву BS 7799, або «Старий Британський стандарт». При розробці стандарту ставилося завдання забезпечення державних та комерційних організацій інструментом для створення і реалізації ефективних систем інформаційної безпеки на основі сучасних інформаційних технологій та методів менеджменту. У 2000 р. на базі BS 7799 був розроблений новий стандарт, що визнаний міжнародним, під назвою «International Standard ISO/IEC 17799 (Information technology - Code of practice for information security management)».

ISO (Міжнародна Організація по Стандартизації) і IEC (Міжнародна Електротехнічна Комісія) формують спеціалізовану систему всесвітньої стандартизації. Національні органи, які є членами ISO або IEC, беруть участь у розробці Міжнародних Стандартів через технічні комітети, створені відповідною організацією з метою роботи з специфічними областями технічної діяльності. Технічні комітети ISO й IEC співпрацюють в областях взаємного інтересу. Інші урядові й неурядові міжнародні організації, пов’язані з ISO й IEC, також беруть участь у цій роботі. На даний час сформовано цілий ряд стандартів ISO/IEC з урахуванням їх впровадження у галузь «Інформаційної безпеки»: ISO/IEC 15408 «Критерії оцінювання безпеки інформаційних технологій», а також стандарти серії 27000 – 27001:2005, 27005:2008, 27006:2007, 27003, 27004, 27007, 27022, 27033.

У даному розділі розглянемо стандарт ISO/IEC 17799, як найбільш поширений та загальний стандарт для організації системи захисту інформаційних ресурсів та сервісних послуг в інформаційно-комунікаційних системах та мережах.

Стандарт ISO/IEC 17799 - це модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки

планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки.

У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої - скорочення матеріальних втрат, пов'язаних з порушенням безперервності бізнесу компанії.

Основна ідея стандарту - допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних й процесу їх обробки згідно визначених послуг та вимог.

Основна структура стандарту

Структура стандарту дозволяє вибрати засоби управління, які мають відношення до конкретної організації або сфери відповідальності у середині організації. Зміст стандарту має такі розділи:

- політика безпеки;
- організація захисту;
- класифікація ресурсів та контроль;
- безпека персоналу;
- фізична безпека та безпека навколишнього середовища;
- адміністрування комп'ютерних систем та обчислювальних мереж;
- управління доступом до систем;
- розробка та супроводження інформаційних систем;
- планування безперервної роботи організації;
- виконання вимог (відповідність законодавству).

У зв'язку з цим виділяється ряд ключових елементів управління, що подаються як фундаментальні:

- політика інформаційної безпеки;
- розподіл відповідальності за інформаційну безпеку;
- освіта та тренінг з інформаційної безпеки;
- звітність за інциденти з безпеки;
- захист від вірусів;
- забезпечення безперервності роботи;
- контроль копіювання ліцензованого програмного забезпечення;
- захист архівної документації організації;
- захист персональних даних;
- реалізація політики з інформаційної безпеки.

Як видно, поряд з елементами захисту та управління для комп'ютерів та комп'ютерних мереж, стандарт велику увагу приділяє питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпеченню безперервності виробничого процесу, юридичним вимогам.

6.4 Задачі організації безпеки інформації та інформаційних ресурсів

Забезпечення безпеки інформаційних мереж - запобігання ушкодженню інформаційних активів і переривання дій, пов'язаних з реалізацією безперервного процесу бізнесу. Інформаційні ресурси та засоби обробки, поширення інформації повинні бути керовані й фізично захищені.

Повинні бути встановлені відповідні експлуатаційні процедури для захисту

документів, носіїв інформації (стрічок, дисків, флешек, касет), обчислювальної техніки, даних, систем введення/виводу й системної документації, які стосуються процесів ушкодження, злодійства й несанкціонованого доступу або інших зловмисних дій.

З даної точки зору необхідно розглядати такі заходи:

- фіксація попереднього змісту інформації, яка повинна бути вилучена з організації та розташована на будь-яких носіях багаторазового користування;

- дотримання строгої авторизації всіх носіїв інформації, що видаляється із організації, а також проведення реєстрації всіх видалень для підтримки процедур аудиту;

- носії інформації повинні зберігатися в надійному, безпечному середовищі, відповідно до встановлених вимог.

Всі процедури й рівні авторизації повинні бути чітко задокументовані. Процедури обробки й зберігання інформації варто встановлювати для того, щоб захистити інформацію від неавторизованого розкриття або неправильного впровадження.

Варто встановити процедури для обробки інформації, відповідно до її класифікації у документах, обчислювальних системах, мережах, мобільних засобах зв’язку, пошті, мовній пошті, мовному зв’язку взагалі, системах з комп'ютерним поданням інформації, поштових послугах/засобах обслуговування, при використанні факсів і будь-яких інших чутливих об'єктів, наприклад, чистих чеків, рахунків.

Заходи управління обробкою й зберіганням інформації :

- обробка й маркування всіх носіїв інформації;

- обмеження доступу при ідентифікації неавторизованого персоналу;

- підтримка офіційної реєстрації авторизованих одержувачів даних;

- забезпечення впевненості в тому, що введені дані є повними та обробка завершується належним чином, а також є підтвердження виводу даних;

- захист (записаних у буфер) даних, що очікують виходу на рівень сумісний з їхньою відповідністю;

- зберігання носіїв інформації в середовищі, що відповідає специфікаціям виготовлювачів;

- відомість розподілу даних до мінімуму;

- чітке маркування всіх копій даних, пропонованих увазі авторизованого одержувача.

Системна документація може містити визначений діапазон інформації, наприклад: опис процесів додатків, процедур, структур даних, процесів авторизації тощо. Необхідно розглянути такі заходи для захисту системної документації від неавторизованого доступу та використання:

- системну документацію варто зберігати згідно з визначеною політикою безпеки та встановленими стандартами;

- список осіб, що мають доступ до системної документації, варто зводити до мінімуму, а авторизацію варто забезпечувати власникові додатків;

- системну документацію, підтримувану загальнодоступною мережею, або отриману через загальнодоступну мережу, варто захищати згідно з визначеною політикою безпеки та встановленими стандартами.

Безпека обміну інформацією й програмним забезпеченням – запобігання

втрат, модифікації або неправильного чи неавторизованого вживання інформації і програмного забезпечення, що підлягає обміну між організаціями та окремими користувачами.

Обмін інформацією й програмним забезпеченням між організаціями та окремими користувачами виконується згідно з встановленими процедурами управління у відповідності чинному законодавству, стандартам або внутрішнім нормативним документам. Обміни варто виконувати на основі угод, або встановлювати внутрішні процедури й стандарти по захисту інформації й носіїв інформації при їх передачі. Дані питання є базовими для процесів безперервності бізнесу і його безпеки з урахуванням питань пов'язаних з електронним обміном даних, електронною торгівлею й електронною поштою, а також вимогами до заходів управління безпекою інформаційних систем.

Угоди обміну програмним забезпеченням повинні включати:

- обов’язки персоналу по управлінню і контролю безпекою та повідомлення про передачу, відправлення й одержання інформації;
- визначені процедури для відправника про передачу, відправлення й одержання повідомлення;
- мінімальну кількість технічних стандартів по формуванню й передачу пакетів;
- стандарти по ідентифікації кур’єра;
- відповідальність й обов’язки у випадку втрати даних;
- використання погодженої системи маркування для чутливої або критичної інформації;
- володіння інформацією й програмним забезпеченням, а також обов’язки по захисту даних, узгодження з авторським правом на програмне забезпечення й аналогічні питання;
- технічні стандарти по запису й зчитуванню інформації й програмного забезпечення;
- будь-які спеціальні засоби управління, які можуть знадобитися, для захисту чутливих об’єктів, таких як криптографічні ключі тощо.

Інформація може бути вразливою до неавторизованого доступу, неправильного вживання або спотворення під час фізичного транспортування, наприклад, при пересиланні носіїв інформації через поштову службу або через кур’єра.

ЛЕКЦІЯ 7. **Забезпечення інформаційної безпеки України**

1. Національна безпека
2. Основні реальні та потенційні загрози інформаційній безпеці України
3. Стан та перспективи розвитку інформаційної безпеки України

1.1 Національна безпека

Необхідною умовою нормального існування і розвитку кожного суспільства є захищеність від зовнішніх і внутрішніх загроз, стійкість до спроб зовнішнього тиску, як здатність протистояти таким спробам і нейтралізувати загрози, що виникають, так і забезпечувати такі внутрішні і зовнішні умови існування країни, які гарантують можливість стабільного і всебічного прогресу суспільства і його громадян. Для характеристики цього стану використовується поняття національної безпеки.

Під **національною безпекою** слід розуміти стан захищеності життєво важливих національних інтересів від внутрішніх і зовнішніх загроз.

Система національних інтересів України визначається сукупністю основних інтересів особи, суспільства, держави і охоплює всі сфери їх діяльності: політичну, економічну, військову, екологічну, інформаційну, науково-технічну, соціальну та інші. Тому в змісті поняття "Національна безпека" можна виділити різні структурні елементи (компоненти), до основних з яких відносяться політична, економічна, військова, екологічна і інформаційна безпека.

Суть **політичної безпеки** полягає в здатності науки створити політичну систему, що забезпечує баланс інтересів різних соціальних груп; самостійно вирішувати питання державного устрою; проводити незалежну внутрішню і зовнішню політику.

Під **економічною безпекою** розуміється стан нації, при якому вона може суверенно, без зовнішнього втручання визначати шляхи і форми свого економічного розвитку.

Військова безпека полягає в можливості забезпечення національної безпеки засобами озброєного насильства. Насамперед військова безпека характеризується здатністю нації стримувати агресію або протидіяти їй.

Екологічна безпека полягає в наявності безпечного місця існування, що забезпечує нормальну життєдіяльність людини. Баланс компонентів у системі "населення - навколишнє середовище - природні ресурси" є гарантом життєздатності людського суспільства.

Інформаційна безпека - стан захищеності інформаційних ресурсів від внутрішніх і зовнішніх загроз, здатних завдати збитку інтересам особи, суспільства, держави (національним інтересам).

Оскільки в умовах інформатизації країни, розвитку інформаційних технологій, інформаційні ресурси формуються у всіх сферах діяльності, і насамперед в політичній, військовій, економічній, науково-технічній, інформаційну безпеку слід розглядати як комплексний **показник** національної безпеки. Цим визначається її важливе місце і одна **з провідних ролей** в системі національної безпеки країни в сучасних умовах. Недарма існує ряд прислів'їв і виразів, що характеризують місце інформації в конкурентній боротьбі і в тактиці військових дій: "Хто володіє

інформацією - той володіє ситуацією", "перемагає той, хто більш інформований про супротивника " та інші.

Основними загрозами інформаційній безпеці є витікання інформації і порушення її цілісності.

Забезпечення інформаційної безпеки здійснюється в рамках забезпечення національної безпеки.

Національна безпека досягається проведенням єдиної державної політики в області забезпечення безпеки, системою заходів економічного, політичного і іншого характеру, адекватних загрозам життєво важливих інтересів особи, суспільства і держави.

Законодавчу основу забезпечення національної безпеки представляють Конституція України, закони України, укази Президента України, ухвали і розпорядження Кабінету Міністрів України, інші нормативно-правові акти державних органів влади і управління, прийняті у межах їх компетенції в даній сфері; міжнародні договори і угоди визнані Україною.

Основним суб'єктом забезпечення безпеки є **держава,** що здійснює функції в цій області через органи законодавчої, виконавчої і судової влади.

До основних **об'єктів** безпеки відносяться: **особа - її права і свободи; суспільство - його матеріальні і духовні цінності; держава - її конституційний лад, суверенітет і територіальна цілісність**.

Громадяни, суспільні і інші організації і об'єднання є суб'єктами безпеки, володіють правами і обов'язками по участі в забезпеченні безпеки.

Принципи забезпечення безпеки.

Основними принципами забезпечення безпеки є:

– законність;

– дотримання балансу життєво важливих інтересів особи, суспільства і держави;

– взаємна відповідальність особи, суспільства і держави по забезпеченню безпеки;

– інтеграція з міжнародними системами безпеки.

Систему національної безпеки утворюють:

– органи законодавчої, виконавчої і судової влади;

– державні, суспільні і інші організації і об'єднання;

– громадяни, що беруть участь в забезпеченні безпеки відповідно до закону;

– законодавство, що регламентує стосунки у сфері безпеки;

– сили забезпечення безпеки.

Для безпосереднього виконання функцій забезпечення національної безпеки в системі виконавчої влади створюються і діють сили і засоби забезпечення національної безпеки.

Сили забезпечення безпеки включають:

а) Збройні сили України; Службу безпеки України;Внутрішні війська; Прикордонні війська України; органи і підрозділи Міністерства внутрішніх справ України; військові підрозділи Міністерства України із питань надзвичайних ситуацій і в справі захисту населення від наслідків Чорнобильської катастрофи; інші військові формування, створені відповідно до Конституції України, які виконують

свої функції в даній сфері згідно чинному законодавству;

б) органи, що забезпечують безпечне ведення робіт в промисловості, енергетиці, на транспорті і в сільському господарстві;служби забезпечення безпеки засобів зв'язку і інформації;митні служби; природоохоронні служби; органи охорони здоров'я населення і інші державні органи забезпечення безпеки, які діють згідно законодавству України.

Для розгляду питань внутрішньої і зовнішньої політики в області забезпечення безпеки, стабільності і правопорядку створено Центральне управління Служби безпеки України, яке відповідає за стан державної безпеки, координує і контролює діяльність інших органів Служби безпеки України.

Центральне управління Служби безпеки України видає положення, накази, розпорядження, інструкції, дає вказівки, обов'язкові для виконання в системі Служби безпеки України. Вказані акти не підлягають виконанню, якщо в них встановлюються непередбачені законодавством додаткові повноваження органів і співробітників Служби безпеки України або антиконституційні обмеження прав і свобод громадян.

У межах своєї компетенції Центральне управління Служби безпеки України вносить Президентові України пропозиції що до видання актів по питаннях збереження державної таємниці, обов'язкової для виконання органами державного управління, підприємствами, установами, організаціями і громадянами.

Забезпечення інформаційної безпеки здійснюється в рамках забезпечення національної безпеки України. Воно передбачає наявність державної системи захисту інформації і законодавства в цій області.

7.2 Основні реальні та потенційні загрози інформаційній безпеці України.

До головних чинників, що впливають на стан морально-ідеологічної стабільності та безпеки в Україні, належать:

- відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади й управління;
- руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку держави;
- повільність процесів усвідомлення прошарком колишньої радянської партійно-господарчої номенклатури, наукової й творчої інтелігенції. паростками нової буржуазії свого місця в суспільстві та формування власне української еліти, що призводить до неможливості сформувати керівними колами зрозумілої й привабливої для суспільства національної ідеї;
- низький загальний рівень розвитку інформаційної інфраструктури, що не виключає ймовірність експансії іноземних компаній на ринку інформаційних послуг; руйнування національного інформаційною простору та виникнення можливості його використання в антидержавних інтересах;
- недостатній професійний, інтелектуальний і творчий рівень вітчизняних виробників інформаційного продукту та послуг, їхня не конкурентоздатність на світовому інформаційному ринку;
- інформаційна експансія провідних іноземних держав, розроблення й використання ними, міжнародними чи вітчизняними злочинними організаціями різних сучасних способів безпосереднього підриву;

- малоконтрольована діяльність окремих політичних сил, ЗМІ та осіб, спрямована на руйнування моральних цінностей, підрив морального й фізичного здоров'я нації; використання ЗМІ з позицій, протилежних інтересам громадян, політичних і громадських організацій, держави:

- втрата довіри до влади з боку значної частини населення внаслідок поширення компромату, застосування «брудних» політичних технологій, особливо під час виборчих кампаній;

- конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації й концентрації інформаційної та політичної влади;

- маніпулювання громадською думкою (шляхом дезінформації, перекручування даних, замовчування правдивих відомостей тощо).

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів влади та управління значно ускладнює прийняття ними зважених. науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах і суспільстві.

Недостатнє інформаційно-аналітичне забезпечення діяльності характерне для всіх державних органів - як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливостей завчасно прогнозувати розвиток подій у державі та навколо неї, належним чином враховувати сприятливі й обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень, здійснювати планування навіть на середньострокову перспективу.

Організація роботи інформаційно-аналітичних підрозділів дотепер не має системного характеру, а в періоди чергових скорочень чисельності державних органів діяльність деяких таких підрозділів взагалі припиняється.

Руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку країни призводить до того, що з огляду на рівень розвитку цієї галузі за кордоном і той факт, що багато держав світу приділяють особливу увагу інформаційній безпеці (створенню спеціальних органів і підрозділів для ведення інформаційних війн тощо). Україна й досі не має достатньої кількості кваліфікованих фахівців. які б змогли на належному рівні ефективно протидіяти інформаційній активності іноземних партнерів щодо її інформаційного простору.

Сучасне українське суспільство, зокрема соціальний прошарок, який має репрезентувати так звану національну українську еліту, поки що перебуває в стані морально-психологічного скніння (відчуваються наслідки ідеологічних диверсій часів холодної війни), ідеологічного й політичного розколу. При цьому процес пошуку загальнонаціональних єднальних моральних та ідеологічних основ стратегії розвитку суспільства відбувається в умовах постійної жорсткої ідеологічної боротьби між іноземними конкурентами за геостратегічні позиції та вплив на правлячі кола України.

Низький загальний рівень інформаційної інфраструктури сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких «засмічують» український інформаційний простір своїм баченням подій, пропагують власний спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство й державу, руйнуючи морально-етичні основи генофонду української

нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його не конкурентоздатність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія надає перевагу російським, американським, ізраїльським, польським, німецьким та іншим іноземним телесеріалам, розважальним й інформаційно-аналітичним програмам.

Недостатній контроль держави за дотриманням законів України політичними силами, ЗМІ й окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, спричиняє непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації, підривання морального й фізичного здоров'я громадян.

У цьому випадку свідомо чи несвідомо ЗМІ створюють додатковий негативний вплив на психіку населення, «готуючи» його до проведення інших заходів прихованого вигідного іноземного впливу.

Втрата довіри до влади з боку значної частини населення відбувається, як уже зазначалося, внаслідок застосування «брудних» політичних технологій. Нині в Україні досить поширена практика оприлюднення «замовних» статей з метою дискредитації окремих громадян і посадових осіб, про яких свідомо розголошуються неправдиві чи конфіденційні відомості. Неправдива інформація і так званий компромат активно поширюються через Інтернет. Для цього навіть створюються спеціалізовані веб-сайти. Розмішена на них інформація поширюється дуже швидко і може завдати моральної чи політичної шкоди громадянам України.

Потенційні можливості для поширення конфіденційної інформації про особу (без її згоди) мають відповідні банки даних, сформовані в довідкових службах, житлово-експлуатаційних конторах, бібліотеках, різних державних органах, лікарнях та інших установах. Наявність таких відомостей створює передумови для протиправних дій, зокрема шантажу громадян.

Нав'язування особі, суспільству бажаних іноземній стороні рішень у життєво важливих сферах суспільної та державної діяльності відбувається шляхом застосування великого арсеналу сил і засобів від ЗМІ до звичайних благодійних організацій, культурних обмінів між державами, а також різних місіонерських структур, що поширюють нетрадиційні релігійні вірування чи окультно-містичні традиції.

Ще одним чинником, який впливає на стан забезпечення інформаційної безпеки, є конкурентна боротьба за володіння ЗМІ та процеси їх монополізації й концентрації інформаційної та політичної влади. В нинішніх умовах боротьба за вплив в електронних і друкованих мас-медіа, за контроль над кінокомпаніями, видавництвами та інформаційними агентствами спричиняє їх зосередження у руках однієї особи чи обмеженого кола людей. Саме це призводить до концентрації влади над споживачами, які одночасно є й виборцями, над політичними партіями та громадськими організаціями, профспілковими об'єднаннями (їм може бути надана підтримка, або з ними боротимуться, або зовсім обійдуть увагою), над іншими видавцями, котрих можна загнати в глухий кут та журналістами, на яких можна «натиснути». Злиття ЗМІ та виникнення монополістичних об'єднань призводить до:

- обмеження можливостей отримання інформації;

- здійснення впливу на свободу дій політичних партій:
- вигідного впливу на діяльність великих і малих видавництв.

Загрози національній безпеці України в інформаційній сфері - сукупність умов та факторів, які становлять небезпеку життєво важливим інтересам держави, суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси й інформаційно-технічну інфраструктуру.

Основними реальними та потенційними **загрозами інформаційній безпеці України** є:

1) *у зовнішньополітичній сфері:*

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують стабільному та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- зовнішні негативні інформаційні впливи на суспільну свідомість і засоби масової інформації, а також Інтернет;

2) у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;
- використання засобів масової інформації, Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;
- несанкціонований доступ до інформаційних ресурсів органів державної влади;
- розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

- порушення встановленого регламенту збирання, оброблення й передавання інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
- реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони України;
- перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;
- інформаційно-психологічний вилив на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

- недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;
- негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

- поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері:

- відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;
- недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;
- несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;
- використання не ліцензованого програмного забезпечення, засобів і комплексів оброблення інформації:
- недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах:

- відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;
- недодержання прав людини і громадянина на отримання інформації, необхідної для захисту їх соціально-економічних прав;
- поширення в ЗМІ не властивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності;
- тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;
- послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;
- відставання розвитку українського кінематографу, книговидання, книго розповсюдження й бібліотечної справи від рівня розвинутих держав;

7) у науково-технічній сфері:

- зниження наукового потенціалу в галузі інформатизації та зв'язку;
- низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;
- відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності;
- недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;
- неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;
- недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій;

- низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування й реагування на надзвичайні ситуації.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами:

- інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для затвердження загальнолюдських та національних моральних цінностей;
- технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації;
- захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності й доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

7.3 Стан та перспективи розвитку інформаційної безпеки України

Інформаційна безпека є одним із видів національної безпеки. Відповідно до законодавства України, інформаційна безпека має таке визначення: "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації".

Інформаційна безпека означає:

– законодавче формування державної інформаційної політики;

– створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

– гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;

– всебічний розвиток інформаційної структури;

– підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;

– створення і впровадження безпечних інформаційних технологій;

– захист права власності всіх учасників інформаційної діяльності в національному просторі України;

– збереження права власності держави нестратегічні об’єкти інформаційної інфраструктури України;

– охорону державної таємниці, а також інформації з обмеженим доступом, що є об’єктом права власності або об’єктом лише володіння, користування чи розпорядження державою;

– створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

– захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

– встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів із іноземними державами;

– законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

У Законі України «Про основи національної безпеки України» визначено основні напрямки державної політики з питань національної безпеки в інформаційній сфері. До них належать:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері,

– наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері створення розвиненого і захищеного інформаційного середовища слугує організація функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які в сукупності становлять об’єкт управління органами державного управління, систему забезпечення інформаційної безпеки, тобто суб’єкт управління, більше того, основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Інформаційна безпека забезпечується комплексом заходів системи

забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян.

Правову основу забезпечення інформаційної безпеки України становлять Конституція України, закони України «Про основи національної безпеки України», «Про інформаційну безпеку України», «Про доступ до публічної інформації», інші закони та інформативно-правові акти, а також ратифіковані або парафовані Україною Договір про безпеку і співробітництво в Європі, Договір «Відкрите небо», Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах.

Лише після революції Гідності питанням інформаційної безпеки приділяється більше уваги. Указом Президента України було оприлюднене рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Було передбачено у місячний термін розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши механізм протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телевізійних каналів, а також запровадження для іноземних засобів масової інформації, системи інформування та захисту журналістів, які працюють у зоні збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп.

У місячний термін також було передбачено за участю Національного інституту та інших органів розробити проект Стратегії розвитку інформаційного простору України і проект стратегії кібернетичної безпеки України, а також розробити комплексні заходи організаційного, інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів із реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилення контролю за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки.

В листопаді 2014 р. було створено Міністерство інформаційної політики. При Міністерстві в процесі спілкування з представниками громадськості була створена Експертна Рада, метою якої стала розробка Стратегії інформаційної політики України, Концепції інформаційної безпеки України та Державної програми розвитку інформаційного простору України.

До пріоритетних напрямків забезпечення інформаційної безпеки України можна зарахувати:

– створення законодавчої та нормативної бази;

– здійснення моніторингу інформаційної безпеки України;

– стандартизація, сертифікація та ліцензування діяльності у сфері забезпечення інформаційної безпеки України;

– удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки України;

– удосконалення системи освіти, навчання та виховання з урахуванням вимог інформаційної безпеки України та Закону України «Про державну мову»;

– розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки України.

На сучасному етапі інтеграційних процесів України до Європейського Союзу особливого значення набуває проблема інформаційного забезпечення політики європейської інтеграції. Завданням інформаційної політики постала необхідність забезпечення вирішення двох основних завдань:

1. Забезпечення загальнонаціональної підтримки курсу інтеграції України в Європейський Союз широкими колами громадськості, створення про європейської більшості в суспільстві.

2.Донесення до урядів і громадськості країн-членів Європейського Союзу об'єктивної інформації про Україну, її досягнень на шляху реформ, створення позитивного іміджу України.

На шляху до вирішення цих завдань постають такі проблеми, які можна вирішити шляхом:

1. Проведення широкомасштабної інформаційної роз'яснювальної компанії серед населення України.

2. Здійснення іноземного просування України в країнах Європейського Союзу.

Проведення планомірного інформування громадськості з питань європейської інтеграції відповідає пріоритетним напрямам Програми інтеграції України до Європейського Союзу. Для забезпечення підтримки політики європейської інтеграції України серед української громадськості необхідно запровадити системи ефективних заходів інформування та освіти суспільства, налагодити механізм співпраці державних органів із засобами масової інформації з метою ефективного використання інформації, яка надходить від центральних органів виконавчої влади, забезпечити прозорість у прийнятті відповідних рішень органів виконавчої влади, налагодити постійний зворотний зв'язок.

Заходи мають охоплювати усі сфери діяльності виконавчої влади. Серед основних заходів, які здійснюються, можна виділити такі освітні заходи:

– розроблення Національної програми перепідготовки й навчання державних службовців центральних, регіональних та місцевих органів влади, спрямованої на поглиблення знань про європейську інтеграцію, забезпечення розуміння цілей інтеграції до Європейського Союзу, його основних інституцій, процесу ухвалення рішень, вміння вести переговори, використовувати європейські інформаційні ресурси, покращення володіння хоча б однією з основних європейських мов;

– інформування молоді з питань інтеграції України до ЄС;

– започаткування у вищих навчальних закладах освітніх програм із інтеграції України до ЄС.

Не менше значення мають видавничі заходи:

– підготовка та видання енциклопедії, словників, серії довідників про ЄС (його історію, законодавство, про держави-члени ЄС), листівок;

– розроблення методичних та довідкових матеріалів на допомогу викладачам, працівникам органів виконавчої влади і органів місцевого самоврядування, присвячених питанням європейської інтеграції;

– виготовлення буклетів, інших пропагандистських матеріалів із висвітленням європейської інтеграції.

Належне місце в інформаційній політиці з питань європейської інтеграції займають комунікативні заходи:

– проведення зустрічей членів Уряду з політиками, представниками центральних, регіональних ЗМІ, громадськістю;

– організація семінарів, брифінгів для представників засобів масової інформації;

– забезпечення виступів керівників у регіонах з окремих питань інтеграції України до Європейського Союзу;

– проведення інтерв'ю, прес-конференцій з питань євроінтеграції;

– організація культурних масових заходів: проведення виставок, конференцій, акцій, форумів, показ високоякісної європейської продукції;

– створення інформаційних центрів із надання населенню інформаційних та консультативних послуг із питань євроінтеграції;

Важливі завдання реалізації інформаційної політики з питань євроінтеграції стоять перед ЗМІ, зокрема:

– підготовка низки телевізійних проектів, програм, передач, репортажів із країн-членів ЄС та держав-кандидатів на вступ до ЄС про досвід європейської інтеграції, про нові можливості, перспективи, наслідки;

– залучення українських мас-медіа як друкованих, так і електронних, телебачення, радіо, інформаційних агентств до висвітлення різних аспектів української політики та внутрішнього життя через призму інтеграції до ЄС;

– розповсюдження через ЗМІ презентаційних та довідкових матеріалів із питань європейської інтеграції України;

– забезпечення участі керівників міністерств, інших центральних органів виконавчої влади в теле- і радіо передачах із метою роз'яснення політики України з питань європейської інтеграції;

– створення веб-сторінок органів виконавчої влади, присвячених питанням європейської інтеграції, та забезпечення розміщення в Інтернеті повідомлень у рамках європейських процесів;

– проведення Інтернет-конференцій із залученням зацікавлених міністерств, інших центральних органів виконавчої влади.

Виконання цих заходів дасть змогу поліпшити знання суспільства про сутність європейської інтеграції, специфіку функціонування ЄС, подолати психологічний пострадянський бар'єр суспільної думки стосовно нової системи європейських координат й інтеграційних перспектив, забезпечити всебічну підтримку Уряду українським суспільством. За цього важливого значення набувають знання про ЄС та виховання молодих людей у дусі спільних європейських цінностей та ідеалів. Звичайно, виконання цих усіх заходів потребує значних фінансових витрат.

Високою буде ефективність від організації просування України в країнах Європейського Союзу та від розроблення структурної програми просування України на міжнародному рівні в процесі інтеграції до ЄС. Український імідж за кордоном має суттєвий вплив на реалізацію цілей української зовнішньої політики у напрямку інтеграції до ЄС. Дуже важливим є формування позитивного національного іміджу,

зокрема в країнах-членах Європейського Союзу. Україна має переконати європейську громадськість, насамперед чиновників Європейської Комісії, що вона гідна посісти чільне місце в стабільній демократичній Європі. Україна зацікавлена в лібералізації зовнішньоекономічних зв'язків з іншими країнами-членами ЄС. Для того, щоб співпрацювати з ними та формувати зону вільної торгівлі, що сприятиме інтенсифікації господарських взаємовідносин, активному обміну капіталом, товарами, послугами, робочою силою, необхідно вирішити багато проблем, одна з яких – забезпечити європейську громадськість повною та вичерпною інформацією про інтеграційну політику України. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України на світовій арені. Успіх переговорів з Європейським Союзом, рівень прийняття європейською громадськістю намірів України щодо входження в ЄС залежить також від результативної діяльності у напрямку просування України серед країн-членів. Для цього теж повинні слугувати відповідні заходи та повинні бути визначені індикатори їх результативності.

В умовах, коли Україна відстоює свій євроінтеграційний курс, проти України розпочато неоголошену війну з боку Російської Федерації. Складовою частиною цієї війни є контрпропаганда, яка ведеться проти України – справжня інформаційна війна. За останніми даними зараз проходить інформаційна операція на Сході України. Ворог намагається створити розкол між силовими структурами України та волонтерами, між силовими структурами і населення, скеровуються зусилля на зрив мобілізації тощо.

У зв'язку з посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності, недостатніми залишаються обсяги вироблення конкурентного національного інформаційного продукту. Наближається до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій.

Забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави передбачає забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства.

Отже, у сучасних умовах важливою складовою національної безпеки є інформаційна безпека України, що є станом захищеності національних інтересів у інформаційній сфері.

ЛЕКЦІЯ 8. **Система та політика забезпечення інформаційної безпеки України. Інформаційна безпека України у сфері прав і свобод людини**

1. Нормативно-правове підґрунтя
2. Мета функціонування, завдання системи забезпечення інформаційної безпеки
3. Політика інформаційної безпеки і її реалізація в Законодавстві України
4. Методи та заходи забезпечення інформаційної безпеки України
5. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя

8.1 Нормативно-правове підґрунтя.

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері. Система забезпечення інформаційної безпеки України (СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління. Формування СЗІБ має відбуватись за усвідомлення необхідності функціонування механізму балансу інтересів усієї системи державного управління в інформаційній сфері. Зазначимо, що за роки незалежності в Україні лише закладено основи для формування системи забезпечення інформаційної безпеки. Так, певним чином можна говорити про напрацювання великого масиву нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України на сьогодні складають: Конституція України, Закон України «Про основи національної безпеки України», інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері.

Нормативно-правове підґрунтя має досить розвинений характер, оскільки більшість норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас, не сформованість нормативно-правової бази щодо регулювання суспільних відносин в сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої і ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері. У Законі України «Про основи національної безпеки України» визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однією з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є вагомою складовою національної.

У найбільш загальному плані під системою забезпечення інформаційної безпеки будемо розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення. Безперечно, можна довго дискутувати з приводу того чи іншого терміну, можна пропонувати численні варіанти, водночас змістовними вони будуть лише тоді, коли будуть визначені основи формування і функціонування СЗІБ. Основами формування і функціонування системи забезпечення інформаційної безпеки є:

- комплексне визначення поняття інформаційної безпеки та її складових елементів, світоглядне та концептуальне закріплення у концепції, доктрині, програмах, планах та інших документах;
- формування і діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування даної системи в цілому;
- формування єдиного методологічного підходу, а також вироблення і прийняття єдиного цілісного і узгодженого законодавства з питань інформаційної безпеки;
- створення чіткого механізму, метою якого була б координація діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління;
- підготовка і забезпечення найкращими професійними кадрами всіх складових елементів підсистеми інформаційної безпеки.

За наявності даних основ можна говорити про їх системну взаємодію, яка забезпечить створення і функціонування чіткої і надійної СЗІБ.

Відповідно до основ формування можна виокремити **основні функції системи забезпечення інформаційної безпеки України.**

1. Створення та забезпечення діяльності державних та недержавних органів та організацій - елементів системи забезпечення інформаційної безпеки, що включає:

- розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);
- системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи державного управління.

2. Управління системою інформаційної безпеки - здійснення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки:

- розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня державного управління;
- здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;
- оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

3. Здійснення планової та оперативної діяльності щодо забезпечення

інформаційної безпеки:

- визначення інтересів органів державного управління в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;
- діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво в сфері інформаційної безпеки:

- розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;
- входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України;
- участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Звичайно, що перелік функцій не є вичерпним, водночас за їх наявності можна говорити про формування певної підсистеми, мета функціонування якої корелюватиме із загальною метою функціонування системи національної безпеки.

Актуальним в контексті розглядуваних проблем вбачається аналіз змісту та призначення системи забезпечення інформаційної безпеки. Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек. Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки. Вживаючи термін «система», робиться логічний наголос на утворенні нової якості, яку складають загрози та небезпеки, суб'єкти забезпечення інформаційної безпеки. Адже структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою і розрив зв'язків між цими елементами може призвести до зникнення самої системи, а отже актуалізується питання забезпечення структурної єдності даної системи. Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності усієї системи інформаційної безпеки органів державного управління. Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи.

У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють струнку організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки. Отже, об'єктами системи забезпечення інформаційної безпеки України є:

- інтереси органів державного управління в інформаційній сфері;

- система органів державного управління, а також їх компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері);
- власне система забезпечення інформаційної безпеки України.

8.2 Мета функціонування, завдання системи забезпечення інформаційної безпеки

Мета функціонування системи забезпечення інформаційної безпеки полягає в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення. У більш загальному плані мета полягає у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави. Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків суспільству й державі.

Головним завданням системи забезпечення інформаційної безпеки України є створення умов для організації управління системою інформаційної безпеки. До основних завдань системи забезпечення інформаційної безпеки належать:

- створення умов для забезпечення інформаційного суверенітету України;
- участь у вдосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- створення умов для активного залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України;
- забезпечення інформаційної безпеки усіх складових елементів системи державного управління;
- забезпечення інформаційно-аналітичного потенціалу країни;
- реалізація державної політики інформаційної безпеки;
- ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки для відпрацювання стратегічних, тактичних і оперативних рішень у сфері державного управління інформаційною безпекою та вироблення механізмів їх реалізації;

- виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;

- виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління;

- моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи державного управління;

- протидія технічному проникненню до інформаційних системи органів державного управління з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;

- запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;

- забезпечення збереження державної таємниці;

- організація демократичного цивільного контролю за функціонуванням системи органів державного управління тощо.

Відповідно до окресленої мети і завдань, доцільно визначити функції системи забезпечення інформаційної безпеки України. Під функціями системи забезпечення інформаційної безпеки розуміємо здійснення суб'єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки. Серед основних функцій системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації слід виділити:

- виявлення і прогнозування загроз життєво важливим інтересам об'єктів інформаційної безпеки, здійснення комплексу оперативних і довгострокових заходів для попередження та нейтралізації загроз;

- створення та підтримання напоготові сил і засобів забезпечення інформаційної безпеки; управління силами і засобами забезпечення інформаційної безпеки в умовах надзвичайної ситуації;

- здійснення системи заходів з відновлення нормального функціонування об'єктів інформаційної безпеки у регіонах, які постраждали внаслідок виникнення надзвичайної ситуації;

- участь в заходах, покликаних забезпечувати інформаційну безпеку за межами України відповідно до міжнародних договорів та угод, укладених або визнаних українською державою.

Враховуючи зазначене, **до основних функцій СЗІБ також можна віднести**:

- розроблення й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства;

- визначення і здійснення повноважень системою органів державного управління щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

- розроблення і реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур в сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;

- розроблення і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;

- здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності органів державного управління;

- введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності органів державного управління (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом);

- забезпечення ефективного використання інформаційних ресурсів у діяльності органів державного управління;

- оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку і ефективного використання інформаційних ресурсів та сприяння доступу уповноважених суб'єктів управління до світових інформаційних ресурсів, глобальних інформаційних систем;

- забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи органів державного управління;

- забезпечення захисту системи державного управління від хибної, спотвореної та недостовірної інформації;

- забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

- регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів;

- кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами; адміністративно-правове забезпечення функціонування системи державного управління;

- інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

- контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

- нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

У межах мети завдань та функцій постає необхідність в окресленні методів і структури системи забезпечення інформаційної безпеки України.

8.3 Політика інформаційної безпеки і її реалізація в Законодавстві України

Державна політика інформаційної безпеки реалізується в рамках політики

національної безпеки і політики інформатизації всіх сфер діяльності держави і суспільства.

Основними напрямами цієї політики є:

- забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси;
- формування і захист державних інформаційних ресурсів;
- створення і розвиток регіональних інформаційних систем і мереж;
- забезпечення національної безпеки у сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації;
- розвиток законодавства у сфері інформаційних процесів, інформатизації і захисту інформації.

Відповідно до цих напрямів в Концепції національної безпеки визначені завдання в області інформаційної безпеки.

Найважливішими завданнями є:

- встановлення необхідного балансу між потребою у вільному обміні інформацією і допустимими обмеженнями її розповсюдження;
- вдосконалення інформаційної структури, прискорення розвитку нових інформаційних технологій і їх широке розповсюдження, уніфікація засобів пошуку, збору, зберігання, обробки і аналізу інформації з урахуванням входження України в глобальну інформаційну інфраструктуру;
- розробка відповідної нормативної правової бази діяльності органів державної влади і інших органів, завдання забезпечення інформаційної безпеки;
- розвиток вітчизняної індустрії телекомунікаційних і інформаційних засобів, їх пріоритетне в порівнянні із зарубіжними аналогами розповсюдження на внутрішньому ринку;
- захист державного інформаційного ресурсу.

Всі напрями політики захисту інформації і інформаційних ресурсів реалізовані в Законодавстві України.

Законодавство в області захисту інформації включає:

- Закон України «Про інформацію»;
- Закон України «Про державну таємницю»;
- Закон України «Про авторське право та суміжні права»;
- Закон України «Про друковані засоби масової інформації (пресу) в Україні»;
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Цивільний кодекс України;
- Кримінальний кодекс України.

В цілому розвиток законодавчої бази в області інформаційної безпеки йде по чотирьох основних напрямах:

- захист відомостей, що складають державну таємницю;
- захист конфіденційної інформації;
- захист авторського права у сфері інформатизації;
- захист права на доступ до інформації.

Основу законодавства складає закон «Про інформацію», який виражає основні напрями політики інформаційній безпеки, суть якоїв своїй основі зводиться до захисту державних інформаційних ресурсів, регулює стосунки, що виникають при

формуванні і використанні інформаційних ресурсів, створенні і використанні інформаційних технологій, захисті інформації, прав суб'єктів, що беруть участь в інформаційних процесах, а також визначає основні поняття, що використовуються в законодавстві.

Органи законодавчої влади (Верховна Рада) видають закони, що регулюють стосунки в області захисту інформації.

Законодавство включає закони. Їх перелік буде розглянутий в ході вивчення тем дисципліни.

Нормативна база формується на основі нормативних правових актів в області захисту інформації, видаваних органами різних гілок влади, міністерствами, відомствами.

Органи виконавчої влади (Уряд) виконують закони. Для цього Уряд приймає відповідні ухвали в області захисту інформації і видає розпорядження, що є підзаконними нормативними правовими актами.

Міністерства і відомства відповідно до свого призначення розробляють і приймають ухвали і рішення, що є нормативними правовими актами свого рівня. Крім того, вони розробляють і затверджують такі нормативні акти як: положення, інструкції, правила, методичні рекомендації.

До нормативних актів цього рівня відносяться також накази і листи керівників відомств і міністерств.

До відомств, що регулюють відносини в області захисту інформації, відносяться:

- Державна служба спеціального зв’язку та захисту інформації України;
- Держстандарт;
- Служба безпеки України;

Окрім цього в забезпеченні інформаційної безпеки беруть участь Служба зовнішньої розвідки (СЗР), Державна прикордонна служба і МВС.

Держстандарт розробляє стандарти в області захисту інформації.

Органи СБУ виконують функції захисту державної таємниці.

Органи МВС ведуть боротьбу з правопорушниками в інформаційній сфері і комп'ютерними злочинами. Для цього в структурі МВС створено спеціальне управління для запобігання і розкриття комп'ютерних злочинів і захисту авторських прав.

Органи Державного митного комітету зобов'язані попереджати незаконне ввезення і вивезення з України "піратської" продукції, забезпечуючи тим самим захист авторських і патентних прав.

Керівники підприємств, організацій, установ, відповідно до своїх посадових обов'язків, при діяльності пов'язаною з інформацією, що складає державну або іншу таємницю, створюють службу (підрозділ) по захисту інформації. Для організації відповідної діяльності вони видають нормативні правові акти: накази, розпорядження; а також затверджують: інструкції, положення, правила, методичні рекомендації, пов'язані із захистом інформації і діяльністю служб захисту інформації.

Для діяльності, пов'язаної з державною таємницею, підприємство повинне мати ліцензію на цей вид діяльності, в його структуру вводиться спеціальний відділ, всі засоби захисту мають бути сертифіковані.

Судова влада здійснює нагляд і притягання до відповідальності за порушення законодавства в інформаційній сфері. У своїй діяльності суди керуються відповідними статтями КК України, ЦК України. Інформаційна безпека є важливою складовою національної безпеки України.

Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону.

Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

- формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку.

Основними завданнями Адміністрації Держспецзв'язку є: забезпечення формування та реалізація державної політики у сферах криптографічного і технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - інформаційно-телекомунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку Національної телекомунікаційної мережі, державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; у сферах захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у таких сферах.

Указом Президента України від 22 жовтня 2021 року № 544/2021 затверджено Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України. Реалізація Концепції розрахована на період до 2025 року та складається з двох етапів. Перший етап (січень 2022 року – грудень 2023 року) зокрема передбачає:

удосконалення з урахуванням міжнародних стандартів та кращих світових практик законодавства України з питань організації та діяльності Державної служби спеціального зв'язку та захисту інформації України, зокрема, у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

розроблення пропозицій щодо скорочення кількості відомчих телекомунікаційних мереж спеціального зв'язку поза межами сектору безпеки і оборони з урахуванням нарощування можливостей єдиної захищеної мультисервісної платформи Національної телекомунікаційної мережі;

удосконалення законодавства України в частині порядку функціонування державної системи урядового зв'язку, процедур внесення клопотань та вирішення питань забезпечення урядовим зв'язком посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ та організацій;

подальший розвиток систем спеціального зв'язку, зокрема в інтересах мережі ситуаційних центрів державних органів, розгортання радіосегмента транспортної платформи Національної телекомунікаційної мережі;

реформування та розвиток систем криптографічного і технічного захисту інформації, протидії технічним розвідкам, проведення оцінки ефективності запроваджених новацій;

започаткування широкого спектра наукових досліджень у сфері кібербезпеки та розробки прикладних систем і засобів кіберзахисту.

Другий етап (січень 2024 року – грудень 2025 року) зокрема передбачає:

модернізацію державної системи урядового зв'язку шляхом інтеграції її мереж в єдину захищену мультисервісну платформу Національної телекомунікаційної мережі та перехід до надання споживачам широкого спектра сучасних сервісів;

переоснащення підрозділів урядового польового зв'язку сучасними цифровими засобами спеціального зв'язку;

модернізацію системи вузлів зв'язку спеціального призначення позаміських пунктів управління державних органів;

завершення розгортання системи оперативно-технічного управління телекомунікаційними мережами в умовах мирного часу, кризових ситуацій, що загрожують національній безпеці, особливого періоду;

забезпечення реалізації новацій законодавства у сфері захисту інформації;

удосконалення системи підготовки фахівців у сфері захисту інформації;

нарощування потужностей з виробництва ключових документів до засобів криптографічного захисту інформації для гарантованого забезпечення потреб державних органів;

впровадження заходів та розроблення засобів кіберзахисту на основі результатів наукових досліджень у сфері кібербезпеки;

впровадження програм короткострокової підготовки (тренування) у сфері кіберзахисту (кібербезпеки) для працівників суб'єктів забезпечення кібербезпеки держави.

У ході реформування Державної служби спеціального зв'язку та захисту інформації України передбачено:

подальшу модернізацію державної системи урядового зв'язку, яка буде

здійснюватися з урахуванням можливостей Національної телекомунікаційної мережі та передбачатиме впровадження нових комплексів спеціального зв'язку, насамперед сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку;

розвиток спроможностей системи урядового фельд'єгерського зв'язку, спрямований на підвищення надійності та оперативності доставки кореспонденції, що містить відомості, які становлять державну таємницю, та/або службову інформацію, офіційної кореспонденції та дипломатичної пошти Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління, закордонних дипломатичних установ України, зокрема шляхом впровадження автоматизованої системи контролю за її проходженням;

розвиток Національної системи конфіденційного зв'язку, який спрямовуватиметься на впровадження механізмів для функціонування ринку конфіденційних послуг; створення захищених точок взаємоз'єднання спеціальних інформаційно-телекомунікаційних систем для забезпечення захищеного міжвідомчого обміну державними електронними інформаційними ресурсами; модернізацію систем для надання сучасних захищених телекомунікаційних послуг IP-телефонії, електронної пошти, Інтернет-доступу, мобільного зв'язку, розгортання та функціонування захищених центрів обробки даних.

Державна система урядового зв'язку – система спеціального зв'язку, що функціонує в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період із забезпеченням додержання вимог законодавства під час передавання, приймання та оброблення інформації, що містить державну таємницю.

Порядок забезпечення урядовим зв'язком посадових осіб державних органів, місцевого самоврядування, підприємств, установ та організацій затверджено Указом Президента України від 18 квітня 2005 року N 663 "Про забезпечення урядовим зв'язком посадових осіб" (для службового користування). Цим же указом затверджено граничну кількість абонентських установок для забезпечення урядовим зв'язком посадових осіб державних органів, місцевого самоврядування, підприємств, установ, організацій та адміністративно-територіальних одиниць. Так, наприклад, в Чернігівській області для визначених окремим переліком абонентів, затвердженим Указом Президента України від 15 лютого 2010 року N 168 "Про переліки абонентів урядового зв'язку" (для службового користування), може бути встановено:

30 абонентських установок міжміського урядового зв'язку;

50 абонентських установок міського урядового зв'язку АТС-100;

10 абонентських установок урядового зв'язку з рухомими об'єктами.

Національна система конфіденційного зв'язку – сукупність спеціальних електронних комунікаційних мереж подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін інформацією з обмеженим доступом, крім інформації, що становить державну таємницю в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану. Послуги конфіденційного зв'язку надаються органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним та фізичним особам.

Фельд'єгерський зв'язок (урядовий фельд'єгерський зв'язок, відомчий фельд'єгерський зв'язок у складі Збройних Сил України) – складова частина поштового зв'язку України, призначена для приймання, обробки, перевезення та доставки (вручення) відправлень, що містять інформацію, яка становить державну таємницю та/або службову інформацію, окремим категоріям користувачів.

Головне управління та підрозділи урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України призначені для організації і забезпечення урядовим фельд'єгерським зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління та інших юридичних осіб відповідно до законодавства.

Основними завданнями Головного управління та підрозділів урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України є:

1) організація, забезпечення і доставка кореспонденції, офіційної кореспонденції та дипломатичної пошти Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління відповідно до переліків, затверджених Кабінетом Міністрів України;

2) доставка кореспонденції, офіційної кореспонденції та дипломатичної пошти Президента України, Голови Верховної Ради України, Прем'єр-міністра України під час поїздок по країні та за кордон, а також виконання особливих доручень;

3) доставка цінних відправлень Кабінету Міністрів України, центральних органів виконавчої влади, Верховної Ради Автономної Республіки Крим та Ради міністрів Автономної Республіки Крим і виконання їх особливих доручень щодо доставки таких відправлень;

4) забезпечення у межах повноважень взаємодії з аналогічними органами держав - учасниць Угоди про Міжурядовий фельд'єгерський зв'язок для збереження та безперешкодної доставки кореспонденції, офіційної кореспонденції та дипломатичної пошти;

5) організація і забезпечення урядовим фельд'єгерським зв'язком державних органів, органів місцевого самоврядування, які не входять до переліків, затверджених Кабінетом Міністрів України, на договірних засадах;

6) проведення заходів з охорони кореспонденції, офіційної кореспонденції та дипломатичної пошти, що доставляється.

Кореспонденція, офіційна кореспонденція та дипломатична пошта, що доставляється урядовим фельд'єгерським зв'язком, є недоторканною, не підлягає розкриттю та/або затриманню, крім випадків, визначених законом.

Порядок забезпечення урядовим фельд'єгерським зв'язком, приймання, доставки, збереження, знищення кореспонденції, офіційної кореспонденції та дипломатичної пошти визначається Кабінетом Міністрів України (затверджений постановою Кабінету Міністрів України від 28 лютого 2018 року № 152).

Поштовий зв'язок спеціального призначення – складова частина поштового зв'язку України, призначена для надання послуг поштового зв'язку окремим категоріям користувачів. Державне підприємство спеціального зв'язку надає послуги поштового зв'язку спеціального призначення: кур'єрські послуги по території

України та послуги з пересилання міжнародних відправлень, доставки цінних відправлень, а також збройного супроводження. Підприємство вже понад 80 років надає унікальні послуги з перевезення всіх видів зброї та боєприпасів, транспортування вибухових та інших небезпечних речовин, перевезення різних цінностей та специфічних медичних препаратів.

Радіочастотний ресурс – частина радіочастотного спектра, придатна для передавання та/або приймання електромагнітної енергії радіоелектронними засобами і яку можливо використовувати на території України та за її межами відповідно до законів України та міжнародного права, а також на виділених для України частотно-орбітальних позиціях. Закон України «Про радіочастотний ресурс України» встановлює правову основу користування радіочастотним ресурсом України, визначає повноваження держави щодо умов користування радіочастотним ресурсом України, права, обов'язки і відповідальність органів державної влади, фізичних і юридичних осіб в цій сфері. План використання радіочастотного ресурсу України – нормативно-правовий акт, яким визначаються напрями використання радіочастотного ресурсу України на даний час та на перспективу. План використання радіочастотного ресурсу України розробляється Центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері користування радіочастотним ресурсом України (ЦОВЗ) згідно з Національною таблицею розподілу смуг радіочастот України на підставі пропозицій і за участю національного регулятора, Національної ради України з питань телебачення і радіомовлення, Генерального штабу Збройних Сил України, інших заінтересованих органів державної влади, а також громадських організацій та суб'єктів підприємницької діяльності. ЦОВЗ подає зазначений План на затвердження Кабінету Міністрів України після його погодження національним регулятором, Національною радою України з питань телебачення і радіомовлення та Генеральним штабом Збройних Сил України. До розгляду питання про затвердження Плану використання радіочастотного ресурсу України на засідання Кабінету Міністрів України обов'язково запрошуються керівники ЦОВЗ, члени національного регулятора, та представники Генерального штабу Збройних Сил України.

8.4 Методи та заходи забезпечення інформаційної безпеки України

Діяльність з забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи.

Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування. Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису та класифікації.

Для здійснення ефективного захисту системи державного управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними. У якості розповсюджених методів аналізу стану забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками,

викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків. Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту.

В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Можна виокремити декілька **типів методів забезпечення інформаційної безпеки:**

- однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;
- багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішенню власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
- комплексні методи - багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

- інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать:

- прийняття рішення з визначення області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній і соціальній сферах життєдіяльності;
- забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи державного управління;
- виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи державного управління;
- трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю з забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз. Саме суспільство частково використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози. Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління по забезпеченню інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління. Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі. Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації органів державного управління. Виконання процедур крипто кодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що працівник органу державного управління буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має

гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Здебільшого забезпечення інформаційної безпеки зводиться до того, що в системних блоках блокується доступ до флоппі-дисків і тим самим унеможливлюється несанкціонований запис інформації. Окрім цього, системний адміністратор встановлює спеціальні програми-фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. Тому не є дивиною, що на сьогодні більша частина українських банків втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського суспільства є те, що жоден з банків жодного разу не визнав факту вчиненого кіберзлочину проти себе. У даному аспекті можна зауважити на ще одну проблему: зневага до вимог інформаційної безпеки та брак необхідних знань. Здебільшого під час робочого дня працівники, виконуючи свої службові обов'язки, відкривають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкривають доступ не лише до інформації, що зараз обробляється, а в цілому до комп'ютерної мережі усієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади.

Отже, важливим методом забезпечення інформаційної безпеки є метод розвитку. Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна та залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторам загроз, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек. Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз та інші. Мета якісної оцінки ризиків - ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них. Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний супротивник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. Причому аналіз подій в світі дає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн. Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно здійснюються оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша - сукупністю

заходів із забезпечення інформаційної безпеки органу державного управління. Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об'єкту безпеки. Метою захисту є переконання супротивника у недоцільності здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на зміну міждержавних відносин, укріплення довіри між державами, створення умов, за яких здійснення небезпечних дій щодо об'єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у супротивника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від супротивника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації. Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного та програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Аналіз проблем забезпечення інформаційної безпеки дав змогу зробити висновок, що найбільш важливими напрямами діяльності у цій галузі є всебічна оцінка загроз та небезпек, національної уразливості, ідентифікація критичної інфраструктури. У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози.

Система забезпечення інформаційної безпеки має бути міжвідомчою та ієрархічно організованою, її структура й організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазису. Потребують подальшого вирішення питання щодо розробки комплексу інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвиток системи сертифікації інформаційних продуктів, систем і послуг, створення системи ліцензування діяльності організацій по окремих напрямах формування єдиного інформаційного простору України.

8.5 Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя

Інформаційна безпека України є однієї зі складових національної безпеки України і впливає на захищеність національних інтересів України в різних сферах життєдіяльності суспільства та держави. Загрози інформаційній безпеці України та методи її забезпечення є загальними для цих сфер. У кожній з них є свої особливості забезпечення інформаційної безпеки, пов'язані зі специфікою об'єктів забезпечення безпеки, ступенем їх уразливості від загроз інформаційній безпеці України. У кожній сфері життєдіяльності суспільства та держави поряд із загальними методами забезпечення інформаційної безпеки України можуть використовуватися часткові методи і форми, зумовлені специфікою чинників, що впливають на стан її інформаційної безпеки.

Забезпечення інформаційної безпеки України в сфері економіки

Забезпечення інформаційної безпеки України у сфері економіки відіграє ключову роль у забезпеченні національної безпеки України. Особлива увага приділяється захисту статистичної, фінансової, біржової, податкової та митної інформації, розробці, впровадженню та стандартизації захищених систем електронних платежів, грошей та торгівлі, та удосконаленню підготовки персоналу для роботи з економічною інформацією.

Забезпечення інформаційної безпеки України в сфері внутрішньої політики

Основними заходами із забезпечення інформаційної безпеки України в сфері внутрішньої політики є створення системи протидії монополізації вітчизняними і закордонними структурами складових інформаційної інфраструктури та активізація контрпропаганди, спрямованої на запобігання негативних наслідків поширення дезінформації про внутрішню політику України.

Забезпечення інформаційної безпеки України в сфері зовнішньої політики

Основними заходами із забезпечення інформаційної безпеки України в сфері зовнішньої політики є розробка основних напрямів державної політики щодо удосконалення інформаційного забезпечення зовнішньополітичного курсу України та створення її представництвам за кордоном умов для роботи з нейтралізації розповсюджуваної там дезінформації про зовнішню політику України.

Забезпечення інформаційної безпеки України у галузі науки та техніки

Найважливішими об'єктами забезпечення інформаційної безпеки України у галузі науки та техніки є: результати фундаментальних, пошукових і прикладних наукових досліджень, потенційно важливі для науково-технічного, технологічного та соціально-економічного розвитку країни. Реальний шлях протидії загрозам інформаційній безпеці України в галузі науки та техніки - це удосконалення законодавства України, яке регулює відносини в цій галузі.

Забезпечення інформаційної безпеки України у сфері духовного життя

Забезпечення інформаційної безпеки України у сфері духовного життя має на меті захист конституційних прав і свобод людини і громадянина, пов'язаних із розвитком, формуванням і поведінкою особистості, свободою масового інформування, використання культурної, духовно-моральної спадщини, історичних традицій і норм громадського життя, збереженням культурного надбання усіх народів України, реалізацією конституційних обмежень прав і свобод людини і громадянина в інтересах збереження та зміцнення моральних цінностей суспільства, традицій патріотизму та гуманізму, здоров'я громадян, культурного та наукового потенціалу України, забезпечення обороноздатності та безпеки України.

Забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах

Основними напрямами забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є запобігання перехопленню, витоку та несанкціонованого доступу до інформації, яка оброблюється чи зберігається в технічних засобах інформатизації, а також ліцензування, атестація і сертифікація об’єктів інформатизації та накладання територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів.

Забезпечення інформаційної безпеки України у сфері оборони

Головними специфічними напрямами удосконалення системи забезпечення інформаційної безпеки України у сфері оборони є виявлення загроз та їхніх джерел, розвиток захищених систем зв'язку і управління військами та зброєю, підвищення надійності спеціального програмного забезпечення та вдосконалення прийомів і способів стратегічного та оперативного маскування, розвідки і радіоелектронної боротьби, методів і засобів активної протидії інформаційно-пропагандистським і психологічним операціям імовірного супротивника.

Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах

Поряд із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки у правоохоронній і судовій сферах - це створення захищеної багаторівневої системи інтегрованих банків даних оперативно-розшукового, довідкового, статистичного і криміналістичного характеру на базі спеціалізованих інформаційно-телекомунікаційних систем та підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем.

Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки

Особливість міжнародного співробітництва України в галузі забезпечення інформаційної безпеки полягає в тому, що воно здійснюється в умовах загострення міжнародної конкуренції за володіння технологічними та інформаційними ресурсами. Основними напрямами міжнародного співробітництва України в галузі забезпечення інформаційної безпеки є заборона розробки, поширення та застосування «інформаційної зброї», забезпечення безпеки міжнародного інформаційного обміну та запобігання несанкціонованому доступу до інформації обмеженого доступу в міжнародних банківських телекомунікаційних мережах і системах інформаційного забезпечення світової торгівлі, до інформації міжнародних правоохоронних організацій, що ведуть боротьбу з транснаціональною організованою злочинністю, міжнародним тероризмом, поширенням наркотиків і психотропних речовин, незаконною торгівлею зброєю та матеріалами, які розщеплюються, а також торгівлею людьми.

Поняття права на інформацію

Забезпечення захисту прав і свобод людини в інформаційній сфері є однією з найважливіших цілей інформаційної безпеки, адже права і свободи людини у сфері інформації є ключовими інститутами громадянського суспільства, правової, демократичної держави, надбанням і цінністю європейської спільноти.

У літературі висловлюються погляди, в яких право громадян на інформацію -

лише складова частина свободи слова та преси, або, навпаки, свобода інформації - умовне позначення цілої групи свобод і прав:

- свободи слова або свободи вираження думок; свободи преси та інших ЗМІ;
- права на одержання інформації, що має суспільне значення;
- свободи поширення інформації.

Вважається, що право на інформацію не охоплюється цілком свободою слова і преси. Воно значно багатіше, змістовніше і має власну субстанцію, грає свою роль у задоволенні певних інтересів суб'єктів; тому зрізаність даного найважливішого права необґрунтовано. Навряд чи виправданий і такий, надмірно широкий, підхід до змісту права на інформацію. Аргументом на користь таких висловлень є, безумовно, законодавча практика найвищого рівня - конституційна. Йдеться, наприклад, про ст. 34 Конституції України, де закріплені не лише свобода думки, слова, але і право на інформацію. Зовсім не випадково закріплені свобода думки і слова та право на інформацію в різних частинах, хоча й однієї статті. Тим самим підкреслюється як їхній взаємозв'язок і взаємопроникнення, так і відома автономність, самостійність, «суверенність». Взагалі, вперше поняття «право на інформацію» було визначено у ст. 9 Закону України «Про інформацію», а саме: «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій». Причому, ст. 1 цього Закону визначає інформацію як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі». Але після набрання чинності Законом «Про телекомунікації», де в прикінцевих положеннях говориться про необхідність узгодження чинного законодавства з положеннями цього нового Закону, поняття інформації визначається вже як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Досить цікавим є також такі **основні положення**, що закріплюються відповідними нормами **Закону «Про інформацію»**:

1. Громадяни мають право доступу до інформації про них, а в період збору інформації мають право знати, які відомості про них і з якою метою збираються, а також оспорювати правильність, повноту, доцільність такої інформації.
2. Право на інформацію охороняється законом.
3. Держава гарантує усім учасникам інформаційних відносин рівні права та можливості доступу до інформації.
4. Інформація не може бути використана з метою, що завдає шкоди правам та свободам громадян України.
5. Не підлягають розголошенню відомості, які становлять державну чи іншу передбачену законом таємницю.
6. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи та законні інтереси інших громадян, права та інтереси юридичних осіб.
7. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

З прийняттям Конституції України в 1996 році, право людини на інформацію -

самостійне конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується ч. 2 ст. 34 Конституції України. Здійснення цього права може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (ч. 3 ст. 34 Конституції України).

Комплекс прав та свобод в інформаційній сфері вважається непорушним та невідчужуваним. За основу положень розділу II «Права, свободи та обов'язки людини і громадянина» Конституції України взято ряд міжнародних нормативно-правових актів. Зокрема, Загальна декларація прав людини, Міжнародний пакт про економічні, соціальні і культурні права, Міжнародний пакт про громадянські та політичні права. У цілому ст. 34 Конституції України відповідає ст. 19 Міжнародного пакту про громадянські і політичні права, який надає кожній людині право вільно шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, та в будь-який спосіб за своїм вибором.

Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина

Крім загального визначення права людини на інформацію в ст. 34 Конституції, є ряд інших інформаційних прав і свобод, що закріплюються конституційними нормами.

1. Свобода особистого і сімейного життя (ст. 32: «...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»);

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: «...винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»);

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це відноситься до відомостей, що «не є державною або іншою захищеною законом таємницею»);

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: «...така інформація ніким не може бути засекречена»);

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками,

встановленими законом»);

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: «...у випадках, передбачених законом, ця допомога надається безоплатно»). Деякі конституційні положення, також мають відношення до інформаційних прав і свобод. Так, за статтями 21, 24 усі люди є вільні і рівні у своєму праві на інформацію, яке є невідчужуваним та непорушним і не залежить від раси, кольору шкіри, релігійних та інших переконань, статі, етнічного та соціального походження тощо. Без отримання необхідної інформації, вільного її використання людина не змогла б розвивати свою особистість (ст. 23).

Право на інформацію пов'язане з правом на свободу світогляду і віросповідання, яке включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноособово чи колективно релігійні культи і ритуальні обряди, вести релігійну діяльність (ст. 35). Реалізація права на освіту (ст. 53) неможлива без вільного інформаційного обміну між людьми. Процес навчання означає, перш за все, пошук і отримання необхідної інформації. Ст. 34 Конституції можна також розглядати як певний розвиток і конкретизацію положення ч. 3 ст. 15, що забороняє здійснення в Україні цензури, тобто обмежувальних заходів щодо здійснення свободи слова в засобах масової інформації. Вона гарантує духовну і творчу свободу, не обмежену ніякою обов’язковою ідеологією. Положення статті гарантують доступ до засобів масової інформації політичним партіям і рухам, громадським організаціям, профспілкам, кожній окремій людині. Ніхто не може бути примушений до зміни чи висловлювання своїх поглядів і переконань. Зрозуміло, що Конституція України закріплює основний зміст прав і свобод в інформаційній сфері, але їх конкретизація відображається в ряді інших нормативно-правових актах.

Структура конституційного права на інформацію

Структура конституційного права на інформацію, що закріплюється Конституцією України та Цивільним кодексом України, визначається такими складовими як:

- збирання інформації;
- зберігання інформації;
- використання інформації;
- поширення інформації.

Відповідно до Закону України «Про інформацію», структурою вищезазначеного права є:

- одержання;
- зберігання;
- використання;
- поширення.

Поняття «збирання» інформації, яке міститься у тексті Конституції, законодавчо не визначено, оскільки Закон України «Про інформацію» дає дефініції тільки таким поняттям як «одержання», «зберігання», «використання» та «поширення». Під одержанням інформації законодавець розуміє набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України. Зберігання інформації — означає забезпечення належного стану інформації та її матеріальних носіїв.

Використання інформації - задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення інформації - розповсюдження, оприлюднення, реалізацію інформації у встановленому законом порядку. Цікавим є той факт, що даний Закон у ст. 38 закріплює також «право власності на інформацію», під яким розуміється «врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією». Отже, законодавець оперує такими поняттями, як «володіння», «користування», «розпорядження», які не визначені законодавчо. Тому, більшість науковців наголошують на необхідності уточнення понять «користування» і «розповсюдження» для з'ясування чіткої різниці між «використанням» і «користуванням» та між «поширенням» і «розповсюдженням» інформації, оскільки фактично використання інформації передбачає і збирання, і поширення інформації, і взагалі будь-які інші маніпуляції з нею. Особливої уваги для забезпечення інформаційної безпеки, заслуговує поняття «доступу до інформації». Ст. 28 Закону України «Про інформацію» містить поняття «режим доступу до інформації» як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Основними положеннями цього Закону згідно зі статтями 28, 29, 30, що закріплюють режим доступу до інформації, є:

1. За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом.

2. Держава здійснює контроль за режимом доступу до інформації.

3. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

4. Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами.

5. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією зацікавлених осіб.

6. Будь-яке обмеження права одержання відкритої інформації забороняється Законом.

7. Інформація з обмеженим доступом поділяється на конфіденційну і таємну.

8. До конфіденційної інформації належать відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб, які можуть поширюватися за їх бажанням відповідно до передбачених ними умов.

9. Таємною є інформація, що містить відомості, які становлять державну та іншу, передбачену Законом таємницю, розголошення якої завдає (чи може завдати) шкоди особі, державі, суспільству.

Відповідно до вимог ст. 37 Закону України «Про інформацію» не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять інформацію:

- визнану у встановленому порядку державною таємницею;
- конфіденційну;
- про оперативну та слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголос може зашкодити

оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;

- що стосується особистого життя громадян;

- щодо внутрівідомчої службової кореспонденції, якщо вона пов'язана з розробкою напряму діяльності установи, з процесом прийняття рішень і передує їх прийняттю;

- що не підлягає розголошенню згідно з іншими законодавчими актами;

- фінансових установ, підготовлену для контрольно-фінансових відомств. Зазначимо, що критерії віднесення інформації до таємної, порядок її обігу та захисту регулюються Законом України «Про державну таємницю».

Оскільки ч. 2 ст. 32 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, то досить цікавим є розгляд цієї проблеми детальніше. Ст. 23 Закону України «Про інформацію» містить такі основні норми:

1. Основними даними про особу (персональними даними) є національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

2. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

3. Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Офіційне тлумачення статті 23 надано Конституційним Судом України у його Рішенні № 5-зп від 30.10.97, де персональні дані про особу віднесені до конфіденційної інформації.

Нормативно-правове забезпечення інформаційної безпеки України.

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України.

Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону ***інформація*** визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Всі громадяни України, юридичні особи і державні органи мають ***право на інформацію***, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав,

свобод і законних інтересів, здійснення завдань і функцій.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Розділ ІІ закону присвячено інформаційній діяльності, під якою розуміється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Визначено основні напрями та *види* інформаційної діяльності – одержання, використання, поширення та зберігання інформації.

У розділі ІІІ закону наведені галузі, види, джерела інформації та режим доступу до неї. Основними галузями інформації визначені: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна.

Основними ***видами інформації*** є: статистична; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

За ***режимом доступу*** інформація поділяється на ***відкриту інформацію*** та ***інформацію з обмеженим доступом***.

Держава здійснює контроль за режимом доступу до інформації.

Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Обмеження права на одержання відкритої інформації забороняється законом.

Інформація з обмеженим доступом за своїм ***правовим режимом*** поділяється на ***конфіденційну*** і ***таємну***.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До ***таємної інформації*** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо),

розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю – це відомості науково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (в тому числі секрети виробництва – так зване ноу-хау), що мають дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці.

Порядок обігу таємної інформації, що не становить державної таємниці, та її захист визначається відповідними державними органами за умов додержання вимог Закону України “Про інформацію”.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Особливим видом таємної інформації є ***державна таємниця***. Вона охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановленому законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається Законом України «Про державну таємницю», яким закладено правову основу створення та функціонування системи охорони державної таємниці в Україні.

Ступінь таємності інформації визначається наданим ***грифом таємності*** «Таємно», «Цілком таємно» та «Особливої важливості».

У розділі IV закону визначені учасники інформаційних відноси, їх права та обов’язки. Основними учасниками цих відносин є: автори, споживачі, поширювачі, зберігачі (охоронці) інформації.

Кожний учасник інформаційних відносин для забезпечення його прав, свобод і законних інтересів має право на одержання інформації про: діяльність органів державної влади; діяльність народних депутатів; діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації; те, що стосується його особисто.

Розділ V закону присвячений охороні інформації, відповідальності за порушення законодавства про інформацію. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації.

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом.

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Розділ VI закону присвячено міжнародній інформаційній діяльності, співробітництву з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації.

Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Стаття 53 закону визначає ***інформаційний суверенітет***. Основою інформаційного суверенітету України є національні інформаційні ресурси.

До ***інформаційних ресурсів України*** входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;
- створенням національних систем інформації;
- встановленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Узагальнена класифікація інформації у відповідності до Закону України «Про інформацію» надана на рис. 8.1.

Рис. 8.1. Класифікація інформації у відповідності до Закону України «Про інформацію»

В ст.10 Закону України «Про основи національної безпеки України» , визначені основні функції суб'єктів забезпечення національної безпеки України (інформаційна сфера окремо не виділена):

- вироблення і періодичне уточнення Стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;
- створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;
- удосконалення її організаційної структури;
- комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) системи;
- підготовка сил та засобів суб'єктів системи до їх застосування згідно з призначенням;
- постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі,

міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

- систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;
- прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;
- розроблення науково-обгрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;
- запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;
- локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;
- оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на ці цілі;
- участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;
- спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у галузі безпеки.

Стаття 11 закону визначає загальні повноваження суб'єктів національної безпеки щодо контролю за здійсненням заходів забезпечення національної безпеки.

Необхідно відзначити, що цей закон був базовим для прийняття "Концепції національної безпеки України". Концепція визначала основні засади державної політики в сфері національної безпеки України та напрями її подальшого розвитку.

В її розділі III «Загрози національній безпеці України» у ряді загроз національній безпеці в інформаційній сфері виділено витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави.

А в розділі IV «Основні напрями державної політики національної безпеки України» для усунення цієї загрози запропоновано розробку і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

У розділі V концепції було сформульовано напрями та заходи для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах створюється система забезпечення національної безпеки України.

Визначена система забезпечення національної безпеки - як організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства України.

Крім того були прийняті Закони України «Про телекомунікації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію», а у Кримінальний кодекс України було введено розділ XVI, в якому визначалася

відповідальність за злочини в інформаційній сфері.

Згодом з’явилася нагальна необхідність в удосконаленні та розвитку як нормативної, так і науково-технічної бази технічного захисту інформації, що й призвело до появи «Концепції технічного захисту інформації в Україні».

У загальних положеннях «Концепції технічного захисту інформації в Україні» визначено основи державної політики у сфері захисту інформації інженерно-технічними заходами. Зокрема визначено, що технічний захист інформації (далі - ТЗІ) є складовою частиною забезпечення національної безпеки України.

Встановлено головні завдання, що повинні вирішуватися концепцією. Концепція має забезпечити єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) і служити підставою для створення програм розвитку сфери ТЗІ.

Також у загальних положеннях концепції визначено, що ТЗІ - це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Показано, що зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку ТЗІ.

Визначено, що напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

При цьому приведення інформаційних відносин у сфері ТЗІ у відповідність з міжнародними стандартами сприятиме становленню України у світі як демократичної правової держави.

У розділі ІІ концепції «Загрози безпеці інформації та стан її технічного захисту» показано, що впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатися

до ліній телекомунікації та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо, радіотехнічної, електронно-оптичної, радіо-теплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок.

За таких умов створилися можливості ***витоку інформації, порушення її цілісності*** та ***блокування***. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, - це одна з основних можливих загроз національній безпеці України в інформаційній сфері. Загрози безпеці інформації в Україні зумовлені:

- не виваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;
- діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;
- недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;
- злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;
- використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ (далі - засоби забезпечення ТЗІ);
- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Стан ТЗІ зумовлюється:

- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;
- недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення ТЗІ;
- незавершеністю створення системи сертифікації засобів забезпечення ТЗІ;
- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;
- недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

У розділі ІІІ концепції «Система ТЗІ» визначено, що ***система ТЗІ*** - *це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами (далі - організаційні структури), нормативно-правова та матеріально-технічна база*.

Зазначено, що правову основу забезпечення ТЗІ в Україні становлять Конституція України, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну

інформацію», інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Принципами формування і проведення державної політики у сфері ТЗІ є:

- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;
- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;
- комплексність, повнота та безперервність заходів ТЗІ;
- відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;
- узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;
- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях (далі - державні органи, підприємства, установи і організації);
- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій;
- покладення відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;
- ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю у межах повноважень, визначених нормативно-правовими актами;
- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
- скоординованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;
- фінансова забезпеченість системи ТЗІ за рахунок Державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Основними функціями організаційних структур системи ТЗІ є:

- оцінка стану ТЗІ в державі, визначення пріоритетних напрямів його розвитку;
- розвиток правових засад удосконалення системи ТЗІ;
- виявлення та прогнозування загроз безпеці інформації;
- забезпечення інженерно-технічними заходами захисту інформації, що підлягає технічному захисту;
- створення умов для ТЗІ, що здійснюється суб'єктами інформаційних відносин

на власний розсуд;

- формування та забезпечення реалізації державної політики щодо створення та впровадження вітчизняних засобів забезпечення ТЗІ;
- створення національної системи стандартизації та нормування у сфері ТЗІ;
- організація фундаментальних і прикладних науково-дослідних робіт та розробок у сфері ТЗІ;
- забезпечення взаємодії організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;
- організація створення та виконання програм розвитку ТЗІ;
- забезпечення ліцензування підприємницької діяльності в сфері ТЗІ;
- організація контролю за якістю засобів забезпечення ТЗІ шляхом їх сертифікації;
- організація контролю за відповідністю вимогам ТЗІ об'єктів, діяльність яких пов'язана з інформацією, що підлягає технічному захисту, шляхом їх атестації;
- організація контролю за ефективністю ТЗІ на об'єктах, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;
- забезпечення підготовки фахівців для роботи у сфері ТЗІ;
- сприяння залученню інвестицій і вітчизняного товаровиробника у сферу ТЗІ;
- організація міжнародного співробітництва в сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;
- забезпечення (кадрове, фінансове, нормативне, матеріально-технічне, інформаційне тощо) життєдіяльності складових організаційних структур системи ТЗІ.

Розділ IV концепції визначає основні напрями державної політики у сфері ТЗІ. Зокрема у ньому прийнято, що державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

Основними ***напрямами державної політики у сфері ТЗІ*** є:

- нормативно-правове забезпечення:
- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;
- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;
- удосконалення правових механізмів організаційного забезпечення ТЗІ;
- удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;
- розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;
- удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації та засобів забезпечення ТЗІ;
- розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;

- розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ:

- у засобах обчислювальної техніки, в автоматизованих системах, оргтехніці, мережах зв'язку, комп'ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту;

- під час створення, експлуатації та утилізації зразків озброєнь, військової та спеціальної техніки;

- під час проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об'єктів;

- організаційне забезпечення:

- забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

- підготовка кадрів для роботи у сфері ТЗІ;

- залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

- розвиток міжнародного співробітництва в сфері ТЗІ;

- науково-технічна та виробнича діяльність:

- моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

- створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

- обґрунтування критеріїв та показників рівнів ТЗІ;

- створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

- створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

- системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

- пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

- створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є:

- створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

- визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;
- визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;
- налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;
- завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;
- визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Значущість забезпечення ТЗІ, його наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади, академій наук.

Слід додати, що одночасно з створенням правових та організаційних основ ТЗІ були створені правові та організаційні основи криптографічного захисту інформації.

У травні 1998 р. прийнято Указ Президента України “Про Положення про порядок здійснення криптографічного захисту інформації в Україні” (відповідно, саме положення було підготовлено дещо раніше).

У липні 2002 року був прийнятий Закон України «Про Національну систему конфіденційного зв'язку», у січні 2003 р. надано розпорядження Президента України «Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку», з дорученням Президента Кабінету Міністрів щодо практичної організації такої системи.

Основні принципи, норми та положення прийнятих законів та підзаконних актів відповідають загальноприйнятим міжнародно-правовим стандартам, в тому числі міжнародним конвенціям з прав людини.

Таким чином, було закладено основні традиції інформаційної безпеки України. Подальший розвиток цієї сфери державного будівництва вимагатиме удосконалення інфраструктури захисту інформації та законів і численних підзаконних актів та нормативних документів, якими регламентується діяльність цієї інфраструктури, а також діяльність органів державного управління, установ та організацій науки й виробництва, які використовують у своїй діяльності інформацію з обмеженим доступом.

На теперішній час в Україні розроблено основна правова та нормативна база, та створена інфраструктура, що має забезпечити надійний захист інформації у державі.

Разом з тим слід пам’ятати, що технічні способи несанкціонованого зняття інформації та засоби протидії цим протиправним діям знаходяться у постійному розвитку.

Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66.
2. Андріяш В. І. Державна політика: концептуальні аспекти визначення. Електронний ресурс. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=626
3. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,;// Гол. ред. Ю. О. Шпак. - К.: "МК-Прес", 2015. - 432 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.— 288 с.
6. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
7. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD) [Електронний ресурс] – Режим доступу: http://www.cbz.com.ua/
8. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD) [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20160304091010/http:/www.cbz.com.ua/resources/files/8510076024d22f2d964df2.pdf
9. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017#Text
10. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
11. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/3855-12#Text
12. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
13. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
14. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.
15. Інформаційна безпека держави: підручник / [В.М. Петрик. М.М. Присяжнюк., Д.С. Мельник та ін.]; в 2 т. Т. 1. / за заг. ред. В.В. Остроухова - К.: ДНУ «Книжкова палата України». 2016. 264 с.
16. Інформаційна безпека України в умовах євроінтеграції: конспект лекцій. Електронний ресурс. – Режим доступу: http://pidruchniki.com/

1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi

17. Карпенко В. Інформаційна політика та безпека: підручник. – Київ, 2006. - Електронний ресурс. Режим доступу: http://ukrlife.org/main/karp/bezpeka15.htm

18. Климчук О. О. Забезпечення інформаційної безпеки держави : підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг. ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України», 2015. – 672 с.

19. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. / [О. О. Климчук, Д. С. Мельник, В. М. Панченко, В. М. Петрик та ін.] ; за заг. ред. В. М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. – 260 с.

20. Конституція України: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Преса України, 1997. – 80 с.

21. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1020

22. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

23. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1032

24. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1030

25. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1031

26. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1050

27. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1036

28. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/919/view/1037

29. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1057_37661772.pdf

30. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та

інформаційно-телекомунікаційних системах» від 29.03.2006 №373 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text

31. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1] [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF-%EF

32. Про Стратегію інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/U685_21?an=4&ed=2021_12_28

33. Технічне завдання на створення автоматизованої системи. ГОСТ 34.602-89 [Електронний ресурс] – Режим доступу: https://www.rts.ua/rus/forpro/613/0/17/