МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Факультет менеджменту

Кафедра економічної кібернетики, комп'ютерних наук та інформаційних технологій

КІБЕРБЕЗПЕКА ТА КІБЕРЗАХИСТ

Конспект лекцій

для здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної форми здобуття вищої освіти

МИКОЛАЇВ
2025

УДК 004.056.5
К38

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного аграрного університету від 27 березня 2025 року, протокол № 7

Укладачі:

О.В.Шебаніна — д-р екон. наук, професор, декан факультету менеджменту Миколаївського національного аграрного університету;

С. І. Тищенко — к.п.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Ю. Пархоменко — к.ф.-м.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О.О. Жебко — асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївського національного аграрного університету;

А.М.Коломієць — асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївського національного аграрного університету;

Рецензенти:

О. С. Садовий - канд. техн. наук, доцент, завідувач кафедри агроінженерії Миколаївського національного аграрного університету

Ю. В. Грицук - канд. техн. наук, доцент кафедри загальної інженерної підготовки Донбаської національної академії будівництва і архітектури

ЗМІСТ

Змістовний модуль 1. Джерела загроз інформації. Класифікація методів і моделей кіберзахисту 4
ТЕМА 1. Основи методології захисту інформації 4
ТЕМА 2. Елементи загальної теорії захисту інформації 18
ТЕМА 3. Джерела загроз інформації 34
ТЕМА 4. Модель захисту та модель порушника в комп'ютерній системі 46
ТЕМА 5. Методи захисту інформації в комп'ютерних системах 53
Змістовний модуль 2. Криптографічний захист інформації. Системи кіберзахисту 65
ТЕМА 6. Методи криптографічного захисту інформації 65
ТЕМА 7. Криптографічні системи з відкритим розподілом ключів 75
ТЕМА 8. Інженерно-технічні методи убезпечення об'єктів інформаційної діяльності 88
ТЕМА 9. Методи відновлення та гарантованого знищення інформації 100
ТЕМА 10. Особливості методів захисту різних видів інформації з обмеженим доступом 118
ТЕМА 11. Елементи управління системою захисту інформації 136
ТЕМА 12. Методика побудови комплексних систем захисту інформації в автоматизованих системах 145
ТЕМА 13. Безпека бездротових мереж 157
РЕКОМЕНДОВАНА ЛІТЕРАТУРА 166

Змістовний модуль 1. Джерела загроз інформації. Класифікація методів і моделей кіберзахисту

ТЕМА 1. Основи методології захисту інформації

Широке використання в процесі інформатизації суспільства сучасних технологій автоматизованої обробки інформації та управління технологічними процесами створило не тільки об’єктивні передумови підвищення ефективності всіх видів діяльності особи, суспільства та держави, але і ряд проблем захисту інформації. Складність вирішення цих проблем обумовлена необхідністю створення систем захисту інформації в умовах обмежених в рамках проектів фінансових, матеріальних, людських та часових ресурсів, використовуючи доступні технології захисту.

В цих умовах розуміння потенціалу різних методів та технологій захисту, їх взаємного зв'язку та взаємного доповнення, глибоке знання принципів та методів управління організаційно-технічними системами створюють надійне підґрунтя ефективного розв’язання згаданих проблем керівниками та виконавцями служб захисту інформації, практиками та дослідниками протягом всього життєвого циклу автоматизованих систем обробки даних.

Сучасний етап розвитку методів обробки інформації, який характеризується інтенсивним впровадженням новітніх інформаційних технологій, поширенням локальних, корпоративних і глобальних мереж у всіх сферах життя цивілізованого держави, створює нові функціональні можливості та забезпечує якість інформаційного обміну.

У зв'язку із цим проблеми інформаційної безпеки набувають першорядного значення, актуальність і важливість яких обумовлена наступними факторами:

- високі темпи росту парку персональних комп'ютерів (ПК), що застосовуються у різних сферах діяльності, і як наслідок, різке розширення кола користувачів, що мають практично необмежений доступ до глобальних обчислювальних мереж і інформаційних ресурсів;
- швидке зростання обсягів інформації, що накопичується, зберігається й оброблюється за допомогою ПК та інших засобів автоматизації;
- стрімкий розвиток апаратних засобів, програмних систем і технологій, що нерідко не відповідають сучасним вимогам з інформаційної безпеки;
- невідповідність стану розвитку засобів обробки інформації й рівня проробления теорії ІБ, розробки правових норм, державних і міжнародних стандартів, що встановлюють вимоги щодо забезпечення необхідного рівня захисту інформації (ЗІ).

Реалії сучасного інформаційного суспільства свідчать, що жодна сфера життя цивілізованого держави не може ефективно функціонувати без розвиненої інформаційної інфраструктури, широкого застосування апаратно-програмних засобів і мережних технологій обробки й обміну інформації, які в свою чергу вразливі відносно новітніх атак на них.

Зазначені вище фактори створюють певний спектр загроз інформаційної безпеки на рівні особистості, суспільства й держави. Нейтралізації значної їхньої частини сприяє формування теорії інформаційної безпеки і методології захисту інформації.

У міру зростання цінності інформації, розвитку й ускладнення засобів її обробки й обміну безпека суспільства все більшою мірою залежить від безпеки використовуваних інформаційних технологій (ІТ). Застосування інформаційних технологій немислимо без підвищеної уваги до питань забезпечення інформаційної безпеки, а інтенсифікація процесів забезпечення інформаційної безпеки – без формування науково-методологічного базису захисту й раціоналізації підходів до створення систем надійного захисту й постійного керування їх функціонуванням.

Методологія захисту інформації як організація продуктивної діяльності людини

Філософія вивчає діяльність як загальний спосіб існування людини. Діяльність людини охоплює матеріально-практичні, інтелектуальні та духовні дії, внутрішні та зовнішні процеси. Діяльність включає як процеси мислення так і рукотворну діяльність.

Діяльність у філософії визначається як активна взаємодія людини з навколишнім середовищем, під час якої людина виступає як суб’єкт, що цілеспрямовано впливає на об’єкт з метою задоволення таким чином деякої потреби.

Суб’єктом є індивід або соціальна група, як носій предметно-практичної діяльності та пізнання, джерело активності, яке спрямоване на об’єкт.

Суб’єкт, з точки зору діалектики, відрізняється притаманним йому самосвідомістю, оскільки він певною мірою опанував створеним людством світом культури: знаряддями практичної діяльності, мовою, логічними категоріями, нормами естетичних та моральних оцінок тощо. Активна діяльність суб’єкта є умовою, завдяки якої той чи інший фрагмент об’єктивної реальності виступає як об’єкт, даний суб’єкту в формах його діяльності.

Об’єкт в філософії означає то, що протистоїть суб’єкту в його професійній діяльності. Об’єкт не тотожній об’єктивної реальності, а виступає як та її частина, що взаємодіє з суб’єктом.

Вчення про організацію діяльності як цілеспрямованої активності людини отримало назву методологія, тобто предметом методології є організація діяльності.

Слід зазначити, що не будь-яка діяльність потребує організації, та, відповідно, застосування методології.

Зокрема, розрізняють два типи діяльності людини: репродуктивну та продуктивну.

Репродуктивна діяльність є копією діяльності іншої людини або власної діяльності, якою опановано внаслідок попереднього досвіду. Така діяльність, як, наприклад, встановлення окремої деталі на виріб, що рухається по конвеєру або проведення щоденної ранкової зарядки загалом вже організована (або самоорганізована) та, вочевидь, не потребує застосування методології.

На відміну репродуктивної діяльності, продуктивна діяльність спрямована на отримання об'єктивно або суб'єктивно нового результату. Зазначимо, що діяльність, наслідком якої є отримання об'єктивно нового результату, є творчістю.

Діяльність, яка у певному сенсі протилежна продуктивної діяльності – це так звана впорядкувальна діяльність. Якщо продуктивна діяльність нерідко руйнує колишні порядки, стереотипи, то впорядкувальна діяльність за суттю спрямована підтримання або відновлення порядку. Вона полягає у встановленні норм діяльності, що подані, зокрема, у формі законів, указів, постанов, наказів, стандартів тощо.

Науково-дослідна діяльність, звичайно, орієнтована на отримання об'єктивно нового результату. Інноваційна діяльність може бути спрямована на об'єктивно новий або на суб'єктивно новий (для конкретного спеціаліста, підприємства, установи, держави) результат. Навчальна діяльність орієнтується на суб'єктивно новий результат для кожної конкретної особи, що навчається.

Саме у випадку продуктивної діяльності внаслідок її складності, багатогранності та не завжди очікуваних результатів виникає необхідність її організації, тобто з'являється потреба у застосуванні методології.

Аналізуючи від діяльності - захист інформації - можливо з’ясувати, що на верхньому рівні (або макрорівні) ця діяльність спрямована на реалізацію кращих методик, практик та попереднього досвіду, основана на впорядкуванні дій та процедур у цій сфері.

Водночас, різноманіття напрямів інформатизації, об’єктів інформаційної діяльності та навколишнього середовища, загроз безпеки інформації та шляхів їх реалізації, неможливість застосування в певних випадках застарілих методик та засобів захисту інформації, що не відповідають викликам сучасності, найчастіше вимагають від фахівця з інформаційної безпеки створення нових технологій та засобів захисту інформації. Це безумовно свідчить, що практична реалізація проектів в сфері інформаційної безпеки має дослідницький продуктивний характер.

Якщо методологію розглядати як вчення про організацію діяльності, то слід з'ясувати зміст поняття «організація». Залежно від визначення та галузі застосування термін організація може означати (рис. 1) три різних сутності:

- властивість, що характеризує внутрішню впорядкованість чогось, узгодженість взаємодії окремих складових цілого, яка обумовлена його структурою або побудовою;

- процес – як сукупність дій або процесів, що призводять до утворення або вдосконалення взаємозв'язків між частинами цілого;

- організаційну систему – як об'єднання людей, що спільно реалізують деякий план, програму або ціль та діють на основі визначених процедур та правил.

Аналізуючи захист інформації, як цілеспрямовану діяльність, ми використовуємо термін «організація» переважно у другому та третьому значенні, тобто як процес або організаційна система. Зауважимо, що у загально філософському змісті поняття організаційна система також використовується для характеристики колективної наукової діяльності, управління проектами тощо.

Виходячи з класифікації діяльності за цільовою спрямованістю: «гра – навчання – праця» розрізняють методологію гри, методологію навчальної діяльності, методологію трудової або професійної діяльності.

Залишаючи поза розглядом специфіку та проблеми навчання та гри, приділімо увагу аналізу трудової діяльності, яку, за звичай, поділяють на практичну діяльність у сферах матеріального або духовного виробництва та специфічні форми професійної діяльності, включаючи науку, мистецтво, релігію.

Організувати діяльність в методології означає впорядкувати її в цілісну систему з чітко визначеними характеристиками, логічною структурою и процесом її здійснення - часовою структурою. При цьому дослідники виходять з пари категорій діалектики: «логічне та історичне (часове)».

Компонентами логічної структури захисту інформації, рівно будь якого іншого виду цілеспрямованої діяльності, є вісім наступних категорій:

суб’єкти діяльності – власники та розпорядники автоматизованих систем, замовники та виконавці робіт зі створення систем захисту інформації, користувачі та обслуговуючий персонал автоматизованих систем тощо;

об’єкти діяльності – загалом глобальні, корпоративні та локальні інформаційні та телекомунікаційні системи та мережі, вузли комутації інформаційних потоків, окремі автоматизовані системи або виділені автоматизовані робочі місця, стаціонарні та рухомі приміщення у яких обробляється та циркулює інформація, що підлягає захисту;

предмет діяльності - зафіксовані досвідом та включені в процес практичної діяльності людини властивості та відношення об’єктів, що досліджуються з певною метою в деяких умовах та обставинах, включаючи: електрична, магнітна, електромагнітна, світлова, акустична та хімічна взаємодії, внаслідок яких відбувається корисний перенос або збереження деякої інформації, а також можуть утворюватися не бажані канали витоку інформацію та впливу на інформацію;

а також чотири сутності - форми, засоби, методи діяльності із захисту інформації та її результат, які детально розглядаються в наступних розділах.

Умовно формулу реалізації діяльності із захисту інформації можливо визначити наступним чином: суб'єкт в рамках деякого об'єкту впливає на предмет діяльності із застосуванням відповідних форм, методів та засобів захисту для убезпечення цінного для нього інформаційного ресурсу, досягаючи внаслідок цього певного результату.

Ефективність діяльності залежить не тільки від її конкретної структури, на неї суттєво впливають зовнішні фактори. До зовнішніх факторів реалізації діяльності слід віднести наступні характеристики: принципи, норми, умови та особливості.

Тут принципи (лат. Principium - основа) – це первоначала, керівна ідея, основне правило поведінки. Наприклад, головний принцип забезпечення надійного криптографічного захисту інформації полягає у створенні криптосистем, безпека яких базується на збереження у секреті ключа, а не алгоритму перетворення.

Норми – це якісні та кількісні характеристики предмету діяльності. Наприклад, для цілей захисту інформації використовуються норми для радіозавад та побічних електромагнітних випромінювань, які встановлюють граничні значення рівнів випромінювань, що виражені в певних фізичних одиницях вимірювання.

Умови та обмеження зовнішнього середовища суттєво впливають на результативність діяльності. Тому під час будь-якої діяльності, у тому числі із захисту інформації слід враховувати наступну сукупність груп умов та обмежень, яка у випадку кожного конкретного виду діяльності може мати власну специфіку та пріоритетність, а саме:

- інформаційні умови;
- кадрові умови;
- матеріально-технічні умови;
- мотиваційні умови;
- науково-методичні;
- нормативно-правові умови;
- організаційні умови;
- фінансові обмеження.

Для кожної епохи в історії людства характерний власний тип культури організації діяльності. Сучасному світу притаманний проектно-технологічний тип культури організації діяльності, сутність якого полягає у тому, що продуктивна діяльність людини або організації поділяється на окремі завершені цикли, що називаються проектами.

При цьому процес здійснення діяльності розглядається у рамках проекту, що реалізується за певною часовою послідовністю по фазах, стадіях та етапах.

Реалізація циклу діяльності – проекту - визначається наступними фазами:

1. Фаза проектування, у підсумку якої будується модель створюваної системи та план її реалізації;

2. Технологічна фаза, результатом якої має бути побудована система;

3. Рефлексивна фаза, що завершується оцінкою реалізованої системи та прийняттям рішення щодо необхідності корекції проведених заходів або старту нового проекту.

Підсумовуючи викладене, можливо зробити висновок про доцільність вивчення методології організації діяльності за наступною схемою:

1. Характеристики умов діяльності (у нашому випадку – захисту інформації): принципи, норми, умови та особливості діяльності.

2. Логічна структура діяльності: суб'єкт, об'єкт, предмет, форми, засоби, методи та результат діяльності.

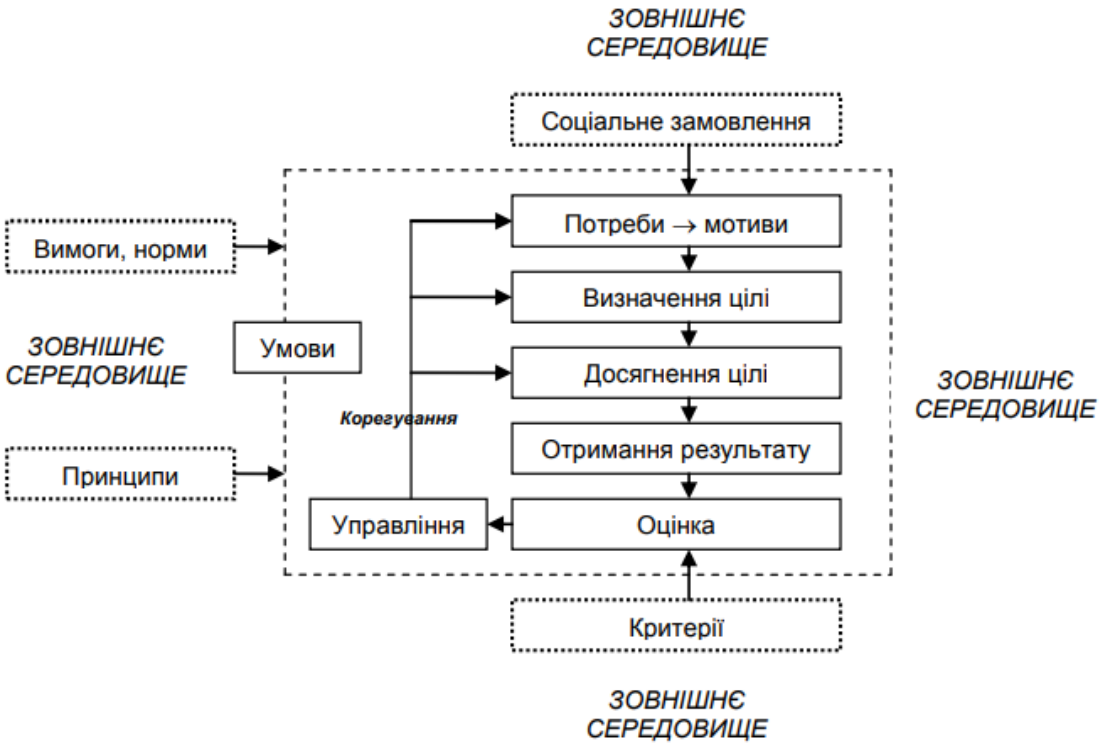
3. Часова структура діяльності: фази; стадії; етапи діяльності.

Оскільки методологію ми розглядаємо як вчення про організацію діяльності людини, доцільно зупинитися саме на основних поняттях, що пов'язані з психологічними та системотехнічними аспектами діяльності.

Діяльність у психології розглядається як найважливіший компонент психіки. Зокрема, науковці вважають що діяльність має входити в предмет психології тому, що психіка не може бути відокремлена від аспектів діяльності, що її породжують.

Системний аналіз за суттю є міждисциплінарним знанням, що розглядає діяльність як складну систему, що спрямована на підготовку, обґрунтування та реалізацію розв'язку складних політичних, соціальних, економічних, технічних та інших проблем.

Співвіднесення підходів цих наукових дисциплін: філософії, психології та системного аналізу (системотехніки) дозволяє побудувати загальну процесну модель діяльності (рис. 2).



Розглянемо основні структурні компоненти діяльності. Відправною точкою моделі є потреби обумовлені нестачею чого-небудь необхідного для забезпечення життєдіяльності людини, соціальної групи, суспільства. Потреби

особи, соціальної групи та суспільства залежать від рівня розвитку даного суспільства, а також від специфічних соціальних умов їх діяльності.

Зокрема необхідність або потреба у обмеженні доступу до певної інформації, у збереженні її незмінної протягом певного часу, у можливості скористатися інформацією тоді, коли в цьому є необхідність – все це є відправним пунктом в організації діяльності із захисту інформації.

Потреби конкретизуються в мотивах, що є ініціаторами діяльності людини, соціальних груп, суспільства. Мотиви обумовлюють цілі як суб'єктивного образа бажаного результату запланованої діяльності.

Ціль є постійним орієнтиром в процесі діяльності, може бути визначена суб'єктом діяльності, або отримана їм зовні.

У випадку репродуктивного (виконавчого) характеру діяльності проблеми визначення цілі не існує, оскільки цілі задаються людині зовні (виконавцю – керівником, учню – вчителем) або цілі не змінюються зовсім, оскільки співробітником щодня виконується одноманітна рутинна робота.

Якщо має місце продуктивна діяльність, навіть відносно нестандартна, то цілі визначаються самим суб'єктом, що може бути доволі складним процесом, якій має власні етапи реалізації, методи та засоби.

В термінах системного аналізу процес визначення цілі має назву проектування.

Процес досягнення мети у кожному конкретному випадку, зокрема під час захисту інформації, має свій зміст, притаманні йому форми, специфічні методи, засоби і технології.

Особливим компонентом даної моделі процес, що має назву саморегуляція, а у випадку колективного суб'єкта, колективної діяльності – управління.

Саморегуляція реалізується у наступний спосіб: прийнята суб'єктом ціль його діяльності → модель умов діяльності → план або програма дій з реалізації → виконання плану → система критеріїв оцінки досягнення мети → дані про реально досягнутий результат → оцінка відповідності досягнутих результатів критеріям успіху → прийняття рішення щодо необхідності та характеру коригування діяльності.

Таким чином, саморегуляція одночасно являє собою з одного боку - замкнений контур регулювання, з іншого - інформаційний процес, носієм якого виступають різні форми відображення дійсності.

Колективна діяльність неможлива без створення певного порядку, розподілу праці, визначення місця і функцій кожного співробітника в колективі, тобто функцій, що реалізуються за допомогою управління. Таким чином, управління розглядається як елемент, функція організованих систем різної природи: біологічних, соціальних, технічних, що забезпечує збереження ними їх певної структури, підтримання режиму діяльності, реалізацію програми, досягнення мети діяльності.

Поняття зовнішнього середовища (рис. 2) є невід'ємною категорією системного аналізу, що розглядає діяльність людини як складну систему.

Зовнішнє середовище визначається як сукупність усіх об'єктів та суб'єктів, що не складають систему, що вивчається, але зміна властивостей або поведінка яких впливає на цю систему, а також тих об'єктів та суб'єктів, властивості або поведінка яких змінюється залежно від поведінки системи.

На рис. 2 окремо виділені фактори, що задаються зовнішнім середовищем: це критерії оцінки відповідності результату поставленій меті; встановлені в суспільстві правові, технічні та інші норми та принципи діяльності.

Матеріально-технічні, фінансові, інформаційні та інші умови діяльності можуть бути віднесені як до зовнішнього середовища, так і до властивостей системи діяльності. Це обумовлюється можливостями активного впливу суб'єкта на створення умов власної діяльності. Наприклад, у випадку браку коштів для реалізації певного проекту існує потенційна можливість залучення інвесторів або спонсорів.

Слід зазначити, що діяльність може здійснюватися шляхом проб и помилок. Методологія же забезпечує перевірені широкою суспільно-історичною практикою раціональні форми організації діяльності.

Понятійний апарат інформаційної безпеки та кібербезпеки

Будь-яка галузь теорії й практики базується на строгому понятійному апараті. Безумовно, формування більш повного переліку термінів, їх визначення й інтерпретація таким чином, щоб забезпечувалося однозначне розуміння кожного з них, має першорядне значення й для розвитку теоретичного базису інформаційної безпеки.

Безліч понять і термінів інформаційної безпеки відображає широкий спектр відмітних істотних властивостей, ознак і відносин, характерних для даного специфічного виду безпеки. У наукових виданнях виділяють три групи термінів теорії інформаційної безпеки. Розглянемо переліки термінів, що входять у відповідні групи.

До першої групи відносять терміни, що визначають наукову основу інформаційної безпеки. Ця група включає терміни, які вживається у багатьох галузях знань і є однозначними, семантично уніфікованими й стилістично нейтральними. Зазначена група, зокрема, включає поняття: інформація, комунікація, конфлікт, вплив, загроза, небезпека, безпека, система.

Терміни цієї групи відповідають вимогам однозначності й стабільності, тобто ці терміни однозначно вживаються в одній галузі знань і зберігають свій особливий зміст у кожній іншій галузі знань, а також є загальновизнаними – вони вживаються в побуті. Однак терміну «інформація» притаманна специфічна властивість: у різних галузях знань, і навіть в одній області знання він може характеризувати предмет, явище, процес і їх властивості й відносини одночасно.

Другу групу утворюють терміни, що визначають об'єкти інформаційної безпеки, в межах яких реалізуються заходи щодо забезпечення інформаційної безпеки в цілому та, зокрема, захисту інформації. Ця група включає поняття: інформатизація, інформаційна система, інформаційні технології, інформаційні

процеси, об'єкт інформаційної діяльності, інформаційний ресурс, інформаційна інфраструктура, інформаційна сфера.

Терміни, що визначають характер діяльності по забезпеченню інформаційної безпеки віднесені до третьої групи. До неї відносяться терміни, що служать позначеннями характерних для цієї сфери предметів, явищ, процесів, їх властивостей і відносин (у тому числі сил, засобів і методів їх використання для розв'язку завдань забезпечення інформаційної безпеки).

Терміни цієї групи позначають широке коло понять різного рівня: від технічного каналу витоку інформації до інформаційного протиборства. До них належать: інформаційне протиборство, інформаційна перевага, інформаційна безпека, загрози інформаційної безпеки, забезпечення інформаційної безпеки, безпека інформації, захист інформації, носій інформації, доступ до інформації, доступність інформації, цілісність інформації, конфіденційність інформації, несанкціонований доступ до інформації, витік інформації, канал витоку інформації, канал передачі інформації, вплив на інформацію, інформаційно-психологічний вплив, інформаційно-психологічна сфера.

Важливою специфічною особливістю термінологічної системи інформаційної безпеки є її тісний зв'язок із правовою лексикою. Це слідство того факту, що інформаційна безпека давно перестала бути лише частиною інформатики та суто технічною дисципліною. У зв'язку із цим формування єдиного розуміння термінології з питань забезпечення інформаційної безпеки створює передумови для цілеспрямованого розвитку теорії інформаційної безпеки й методології захисту інформації.

Визначення інформаційної безпеки у світлі інформаційних проблем сучасного суспільства. Відомо, що кожне явище, процес, об'єкт має внутрішній зміст й зовнішній вираз. Тільки сполучення цих складових дає повне уявлення про предмет дослідження й можливі напрями використання його результатів.

Складність висвітлення проблеми забезпечення інформаційної безпеки пов'язана з відсутністю дотепер загальноприйнятого тлумачення термінів, використовуваних для опису даної предметної області. У зв'язку із цим для визначення поняття інформаційної безпеки необхідно розглянути базове ключове поняття «безпека».

Безпека як загальнонаукова категорія може бути визначена як деякий стан розглянутої системи, за умов якого остання, з одного боку, здатна протистояти дестабілізуючому впливу зовнішніх і внутрішніх загроз, а з іншого – її функціонування не створює загроз для елементів самої системи й зовнішнього середовища. При такому визначенні мірою безпеки системи є:

- з погляду на здатність протистояти дестабілізуючому впливу зовнішніх і внутрішніх загроз – ступінь збереження системою своєї структури, технології й ефективності функціонування у разі впливу дестабілізуючих факторів;

- з погляду на відсутність загроз для елементів системи й зовнішнього середовища – рівень вірогідності появи таких дестабілізуючих факторів, що можуть являти загрозу елементам самої системи або зовнішньому середовищу.

Інтерпретація даних формулювань приводить до наступного визначення: інформаційна безпека – такий стан розглянутої системи, в якому вона, з одного

боку, здатна протистояти дестабілізуючому впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її функціонування не створює інформаційних загроз для елементів самої системи й зовнішнього середовища.

Орієнтиром у напрямку визначення шляхів вирішення проблем інформаційної безпеки може слугувати власне інформація.

Інформація як неодмінний компонент будь-якої організованої системи, з одного боку, легко вразлива (тобто дуже чутлива до дестабілізуючого впливу великої кількості різноманітних загроз), а з іншого – сама може бути джерелом багатьох різнопланових загроз, як для елементів самої системи, так і для зовнішнього середовища.

Звідси, забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуте лише при взаємопов'язаному розв'язку трьох складових проблем:

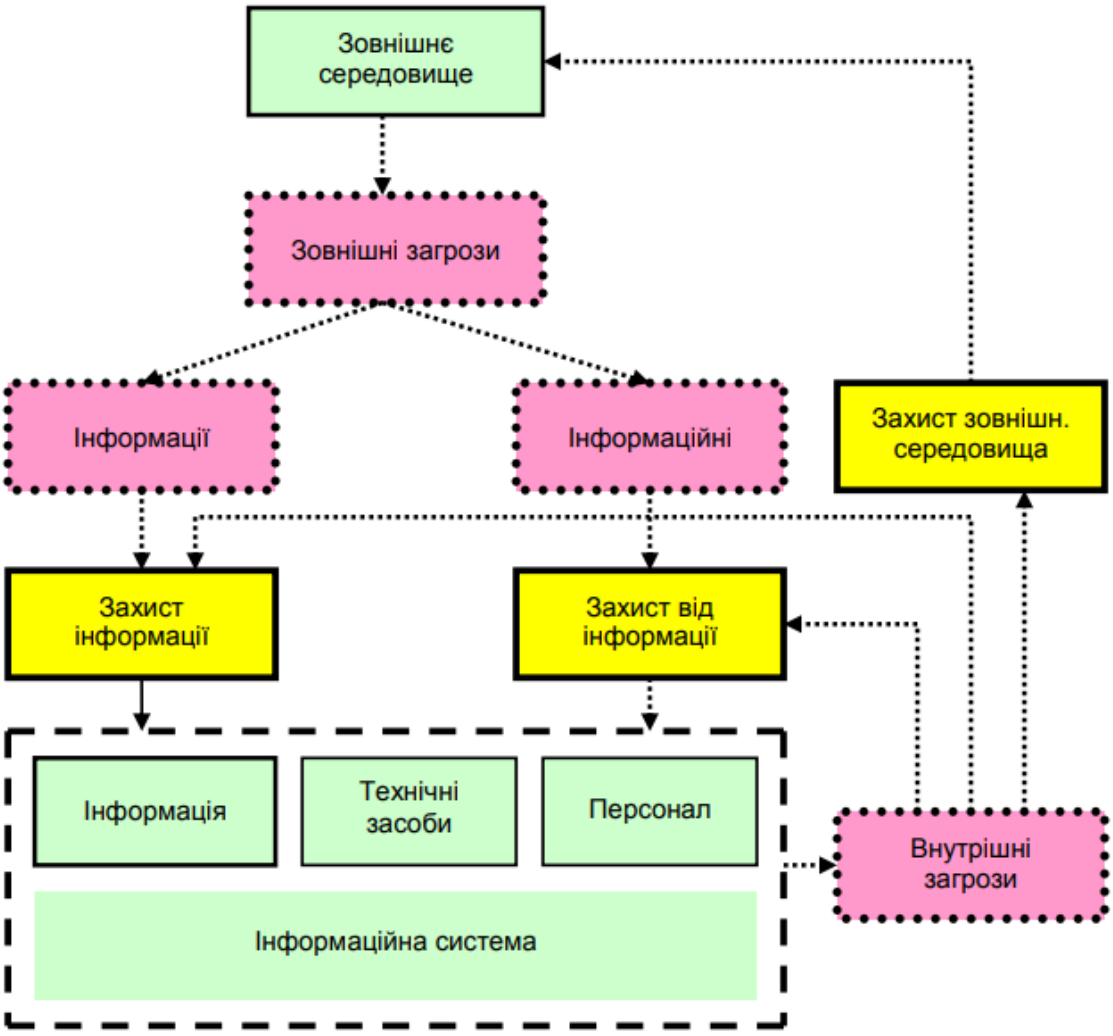
- захист інформації, що перебуває в системі, від дестабілізуючого впливу зовнішніх і внутрішніх загроз інформації;
- захист елементів системи від дестабілізуючого впливу зовнішніх і внутрішніх інформаційних загроз;
- захист зовнішнього середовища від інформаційних загроз із боку системи, що розглядається.

Відповідно до викладеного загальна схема забезпечення інформаційної безпеки може бути представлена так, як показано на рис. 3

З наведеного можливо з'ясувати, що, по-перше, розвиток теорії інформаційної безпеки обумовлюється основними напрямами розвитку теорії захисту інформації як першої складової загальної проблеми інформаційної безпеки. По-друге, розвиток теорії інформаційної безпеки визначається рівнем вивчення і розробки другої складової інформаційної безпеки – захисту від інформації.

Слід акцентувати увагу на складності розв'язання другої складової проблеми інформаційної безпеки, оскільки у цій сфері відчувається певний вакуум у плані концептуальних напрацювань.

Необхідно також зазначити, що проблема захисту від інформації суттєво складніше проблеми захисту інформації внаслідок різноманітності інформаційних загроз, вплив яких не завжди передбачуваний. Запобігання й нейтралізація таких загроз вимагають як розробки та впровадження адекватних технічних рішень, так і організаційно-правових та політичних заходів на державному та міжнародному рівнях.



Ще відмітимо, що характерною рисою проблеми захисту особи та суспільства від інформації, є переважно гуманітарний характер її розв'язання, якій дуже важко піддається формалізації. При цьому розв'язок задач щодо захисту від інформації технічних засобів і систем, так само як і рішення щодо захисту інформації, носять переважно організаційно-технічний характер і піддаються строгій структуризації.

Як випливає з схеми, наведеної на рис. 3, захист інформації виступає деякою подобою захисної оболонки, яка протистоїть дестабілізуючим впливам (видам уразливості інформації) і забезпечує інформаційну безпеку. Суть же цієї оболонки «захист інформації» у тому, щоб забезпечити безпеку самої інформації.

Складові забезпечення інформаційної безпеки та кібербезпеки

Інформаційна безпека багатомірна галузь науково-практичної діяльності, у якій успіх може принести тільки системний, комплексний підхід.

З методологічної точки зору підхід до проблем інформаційної безпеки повинен починатися з виявлення суб'єктів інформаційних відносин і інтересів цих суб'єктів.

У забезпеченні інформаційної безпеки зацікавлені різні суб'єкти інформаційних відносин:

- держава в цілому або окремі державні органі й організації;

- суспільні або комерційні організації, підприємства (юридичні особи);
- окремі громадяни (фізичні особи).

Спектр інтересів суб'єктів, пов'язаних з накопиченням і обробкою інформації, сфокусований на наступних трьох категоріях: забезпечення доступності, цілісності й конфіденційності ресурсів інформаційного середовища й підтримуючої інфраструктури.

Пояснимо суть понять доступність, цілісність і конфіденційність інформації.

Доступність – це властивість інформації, що характеризує можливість за прийнятний час одержати на законних підставах потрібний інформаційний ресурс (послугу).

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування й несанкціонованої зміни.

Конфіденційність – це властивість інформації з обмеженим доступом, яка характеризує її захищеність від ознайомлення з нею осіб, які не мають на це повноважень.

У якості основних інформаційних ресурсів надалі будемо розглядати дані, що оброблюються у автоматизованих (інформаційних) системах за допомогою засобів комунікацій.

Інформаційні системи створюються для реалізації певних інформаційних послуг. Якщо по тим або іншім причинам надати ці послуги користувачам стає неможливо, це, очевидно завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим аспектам, прийнято виділяти її як найважливіший елемент інформаційної безпеки.

Цілісність можна розглядати як статичну, що розуміється як незмінність інформаційних об'єктів, так і динамічну (стосовну до коректного виконання складних дій). Засоби контролю динамічної цілісності застосовуються зокрема при аналізі потоку фінансових повідомлень із метою виявлення крадіжки, модифікації або дублювання окремих повідомлень.

Забезпечення конфіденційності – нормативно найбільш пророблений аспект інформаційної безпеки. Але у практичній реалізації заходів із забезпечення конфіденційності сучасних інформаційних систем є серйозні труднощі.

По-перше, встановлена законом вимога захисту персональних даних нормативно-правовими актами нижчого рівня й технологічно поки ще не забезпечена.

По-друге, відсутні відкриті критерії щодо захисту від витоку конфіденційної інформації по технічних каналах, що ускладнює задачу значної частини власників інформаційно-телекомунікаційних систем по оцінці можливих ризиків від реалізації відповідних загроз.

По-третє, слабке пророблення поняття «службова інформація» не дозволяє диференційовано підходити до її різновидів, При цьому очевидно, що службова (конфіденційна) інформація Міністерства оборони й службова (конфіденційна) інформація Міносвіти мають різну цінову вагу. Це досить часто створює передумови для надмірних фінансових витрат, наприклад, для

придбання апаратних засобів захисту інформації, на шкоду більш дешевим (хоча й менш безпечним) програмним засобам.

Можливо звернути увагу, що значення кожної зі складових інформаційної безпеки для різних категорій суб'єктів інформаційних відносин різне.

Наприклад, у більшості випадків, у державних структурах (крім сфери банківської діяльності) пріоритет віддається конфіденційності.

Дві інших складових інформаційної безпеки - доступність і цілісність інформації – в випадку інформації з обмеженим доступом мають дещо менший пріоритет.

Навпаки, у банківській сфери порядок пріоритетів при здійсненні обробки даних в електронній формі іншій: цілісність, доступність, конфіденційність.

Для комерційних організацій провідну роль відіграє доступність інформації. Особливо яскраво це проявляється в різного роду системах керування – торгівлі, виробництва, транспорту й ін.

Для користувачів систем Інтернет – банкінгу та торгівлі в мережі Інтернет менш драматичні, але також досить неприємні матеріальні і моральні наслідки, може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних і авіаквитків, банківські послуги тощо).

Цілісність також найважливіший аспект інформаційної безпеки комерційних структур. Набір і характеристики комплектуючих виробів, хід технологічного процесу – усе це приклади інформації, порушення цілісності якої може виявитися в буквальнім значенні летальним. У той же час конфіденційність у випадку комерційної інформації відіграє помітно меншу роль.

Для громадян на перше місце можна поставити цілісність і доступність інформації, володіння якої необхідно для здійснення нормальної життєдіяльності. Наприклад, зростання кількості випадків викривлення інформації під час виборів створює певну напругу у суспільстві. Конфіденційність для фізичних осіб відіграє вторинну роль, хоча, як уже відзначене, що фізичні особи на сьогоднішній день є самими незахищеними суб'єктами інформаційних відносин.

Підсумовуючі викладене можливо зробити наступні висновки:

- сучасний етап розвитку суспільства характеризується зростанням ролі інформаційної сфери, що уявляє собою сукупність інформації, відповідної інфраструктури, суб'єктів, які збирають, накопичують, обробляють формують, поширюють інформацію;

- інформаційна сфера як системотворчий фактор життя суспільства активно впливає на стан політичної, економічної, національної, оборонної й інших складових безпеки України. Це потребує адекватного стану інформаційної безпеки та її важливої складової захисту інформації.

Проблеми розвитку теорії і практики забезпечення інформаційної безпеки та кібербезпеки

Сучасний розвиток теорії та практики інформаційної безпеки пов'язаний з новими тенденціями, що характерні для поточного стану інформатизації суспільства.

По-перше, виникнення та розвиток новітнього феномену сучасності – кібернетичного простору, як сукупності взаємно пов’язаних життєво важливих інфраструктур в сфері національної безпеки і оборони, в банківської справі та фінансах, в енергетиці тощо – призвело до активізації досліджень та розробок у сфері невід’ємної складової інформаційної безпеки – кібернетичної безпеки. Зокрема, поступово на державному рівні формується усвідомлення та реалізуються першочергові заходи щодо нормативного врегулювання комплексу проблем в цій сфері та організаційно-технічного забезпечення їх розв’язку.

По-друге, поряд з необхідністю вдосконалення захисту інформації все більшого значення набуває питання захисту суспільства та машино-людинних (головним чином, інформаційних) систем від руйнуючого впливу інформації, тому формується завдання забезпечення інформаційної безпеки як органічної сукупності задач захисту інформації й захисту від інформації.

По-третє, розв'язок завдань захисту інформації та захисту від інформації, обумовлюють підвищені вимоги щодо ефективності діяльності об'єктів інформатизації. Виникає узагальнене поняття управління інформацією, яке поєднує вище позначені поняття, задачі управління інформацією мають бути враховані при формуванні концепції інформаційного забезпечення діяльності суб'єктів інформаційного суспільства.

По-четверте, поточний етап розвитку теорії захисту інформації потребує прискіпливої уваги питанням вдосконалювання науково-методологічного базису й інструментальних засобів, що забезпечують на регулярній основі розв'язок будь-яких виникаючих задач в органічному зв'язку з вирішенням проблем інформаційної безпеки, впровадження новітніх інформаційних технологій, поступової інформатизації суспільства.

Таким чином, вище викладене дозволяє виділити наступні найбільш гострі проблеми розвитку теорії й практики інформаційної безпеки. Такими є:

- створення теоретичних основ і формування науковометодологічного базису, що дозволяють адекватно описувати процеси в умовах значної невизначеності й непередбачуваності прояву дестабілізуючих факторів (інформаційних загроз);

- розробка науково-обґрунтованих нормативно-методичних документів з питань забезпечення інформаційної та кібернетичної безпеки на базі дослідження й класифікації загроз інформації й вироблення стандартних вимог до захисту;

- стандартизація підходів до створення систем захисту інформації й раціоналізація схем і структур управління захистом на об'єктовому, регіональному й державному рівнях.

Розв'язок спектра перерахованих завдань має велике значення для реалізації положень Концепції національної безпеки України.

ТЕМА 2. Елементи загальної теорії захисту інформації

Характеристика інформації як об’єкта захисту

Інформація, що включає відомості про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання, як предметом захисту має низку особливостей, зокрема:

- вона нематеріальна;
- інформація зберігається й передається за допомогою матеріальних носіїв;
- будь-який матеріальний об'єкт може містити інформацію про себе або інші об'єкти.

Нематеріальність інформації розуміється в тому сенсі, що не можна виміряти її параметри відомими фізичними методами й приладами. Інформація не має маси та енергії.

Найбільш важливою властивістю інформації, з погляду захисту інформації, є її цінність. Цінність інформації визначається ступенем її корисності для власника.

Існує чимало підходів до формалізації процесу оцінки цінності інформації, однак дотепер в цьому процесі залишається значна частка суб'єктивізму.

Володіння дійсною (достовірною) інформацією дає її власникові певні переваги. Дійсною або достовірною інформацією вважається інформація, яка з достатньою для власника (користувача) точністю відображає об'єкти й процеси навколишнього світу в певних часових і просторових рамках.

Недостовірна, перекручена інформація, що свідомо спотворює дійсність, може нанести отримувачу або її розпоряднику значний матеріальний і моральний збиток. Зазначимо, що викривлена навмисно інформація отримала назву дезінформація.

Законом «Про інформацію» гарантується право власника інформації на її використання й захист від доступу до неї інших осіб (організацій)

Головним м критерієм для ухвалення рішення про обмеження доступу до інформації та щодо способів її убезпечення є цінність цій інформації.

Існує два основних підходи щодо убезпечення інформації. Перший підхід реалізується шляхом захисту інформації від її витоку, руйнування або блокування у комп’ютерних системах та інших фізичних середовищах, коли носієм інформації виступають фундаментальні явища природи: електричні, магнітні, електромагнітні, оптичні та хімічні процеси.

Другій підхід реалізується шляхом охорони інформації. При цьому на відміну від захисту інформації, охороні підлягає тільки документована інформація, тобто інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати.

З урахуванням права власника інформації обмежувати доступ до неї, документована інформація з обмеженим доступом (ІзОД) за умовами її правового режиму поділяється на відкриту та конфіденційну інформацію, а

також різного роду таємниці: адвокатську, банківську, державну, комерційну, лікарську, нотаріальну.

Відповідно до Закону «Про державну таємницю» державну таємницю можуть містити відомості, що належать та представляють цінність для держави, Таким відомостям може бути встановлено один із трьох можливих ступенів обмеження доступу: «таємно», «цілком таємно», «особливої важливості».

Ступінь обмеження доступу – це адміністративний або законодавчий захід, відповідно до міри відповідальності особи за витік або втрату конкретної інформації з обмеженим доступом, що регламентована спеціальним документом, з урахуванням державних, військових, стратегічних, економічних, комерційних, службових інтересів.

Конфіденційні відомості, що належать державі, отримали назву службової інформації. Переліки службової інформації затверджуються в кожному державному органі наказами відповідних посадових осіб.

Адвокатську, банківську, комерційну. лікарську, нотаріальну таємницю можуть містити відомості, що належать приватній особі, підприємству, установі, корпорації тощо.

Необхідно зауважити, інформація має властивість адитивності, об'єднання (збільшення обсягу) різноманітної інформації підвищує в загальному випадку її цінність, сумарна сукупність проаналізованої та певним чином впорядкованої відкритої інформації може перевести її в категорію службової, узагальнені службові відомості в остаточному підсумку можуть виявитися секретними.

Цінність інформації змінюється в часі. Як правило, з часом цінність інформації зменшується. Залежність цінності інформації від часу приблизно визначається згідно з рівнянням:

$$C(t)=C_0 10^{-t/\tau},$$

де С0 – початкова цінність інформації (в момент її виникнення або одержання);

t – час від моменту виникнення інформації до моменту визначення її вартості;

τ– час від моменту виникнення інформації до моменту її остаточного старіння.

Час τ в формулі, через який інформація стає застарілою, міняється в дуже широкому діапазоні. Так, наприклад, з погляду диспетчерських служб у авіації, дані про положення літаків у просторі застарівають за лічені секунди. У той же час інформація про закони природи залишається актуальною протягом багатьох тисячоліть.

Інформація купується й продається. Її правочинне розглядати як товар, що має певну ціну. Ціна, як цінність інформації, пов'язана з корисністю інформації для конкретних людей, організацій, держав.

Інформація може бути коштовною для її власника, але непотрібною для інших. У цьому випадку інформація не може бути товаром, а, отже, вона не має й ціни.

Інформація може бути отримана шляхом:

- проведенням наукових досліджень;
- покупкою інформації;
- протиправним добуванням інформації.

Як будь-який товар, інформація має собівартість, яка визначається витратами на її одержання. Собівартість залежить від вибору шляхів одержання інформації й мінімізації витрат при добуванні необхідних відомостей обраним шляхом. Інформація може добуватися з метою одержання прибутку або переваг перед конкурентами. Для цього інформація:

- продається на ринку;
- впроваджується в виробництво для одержання нових технологій і товарів, що приносять прибуток;
- використовується в наукових дослідженнях;
- дозволяє приймати оптимальні рішення в управлінні.

Було зазначено що обсяг інформації впливає на її цінність. Зауважимо, оцінки кількості інформації у одиницях двійкового її подання в кілобайтах (1 Кб=1000 байт), мегабайтах (1 Мб=10^6 байт), гігабайтах (1 Гб=10^9 байт), і, навіть, в терабайтах (1 Тб=10^{12}байт) не можуть дати нам реальної картини щодо кількості інформації на конкретному носії с точки зору її цінності. Причина цього, зокрема, обумовлюється наявністю в поданні інформації певної надлишковості, дублювання відомостей та присутності очевидних фактів.

Наприклад, наявність надлишковості в письмових повідомленнях дозволяє скоротити довжину тексту «Інформаційне повідомлення доставлене» на третину завдяки пропуску голосних літер: «Нфрмцн пвдмлнн дствлн» практично без втрати змісту. Тобто більш коротке повідомлення має таку саму цінність, як і більш довге.

Дублювання інформації може бути в явному вигляді в разі передавання по каналу зв’язку елементів графічних форм подання інформації, повторення одиниць виміру тощо, так і у неявному вигляді, що обумовлене логічними зв’язками між окремими елементами повідомлення, наявність яких дозволяє зробити вірні висновки.

Наприклад, у повідомлення «Швидкість вітру у районі аеропорту перевищує 40 м/сек. Виліт усіх рейсів відмінений» друге речення для спеціаліста є зайвим. В цьому випадку в першому реченні фактично мова їде про потужний шторм в районі аеропорту. Друге речення для спеціаліста вже не містить інформації, оскільки для більшості цивільних літальних апаратів заборона на зліт наступає у випадку втричі меншої швидкості вітру з будь яких напрямків.

Очевидний факт ми бачимо, наприклад, в повідомленні «В січні температура повітря в районі Північного полюсу не зростає вище відмітки 0 оС», воно не містить інформації для освіченої людини та не має цінності.

Таким чином, існує проблема складності об'єктивної оцінки кількості інформації. Для виміру кількості інформації використовують декілька різних за суттю підходів.

І. Ентропійний підхід базується на математичних методах теорії інформації. У теорії інформації кількість інформації оцінюється мірою

зменшення в одержувача невизначеності (ентропії) вибору або очікування подій після одержання інформації. Кількість інформації тим більше, чим нижче ймовірність настання події.

Цей метод широко використовується при визначенні кількості інформації, що передається по каналах зв'язку. При прийманні інформації здійснюється вибір між символами алфавіту в прийнятому повідомленні.

Нехай повідомлення, прийняте по каналу зв'язку, складається з N символів. Тоді кількість інформації I в повідомленні, без урахування зв'язків між символами в повідомленні, може бути розрахована по формулі, що запропонована американським математиком Клодом Шенноном:

$$I = -N\sum_{i=1}^{n} P_i \cdot \log_2 P_i, ,$$

де Pi – імовірність появи в повідомленні символу з номером і,

n – кількість різних символів в алфавіті мови.

Нехай, наприклад, для передачі повідомлень використовуються лише чотири символи {A,B,C,D}, що зустрічаються з ймовірністю:

PA=1/2, PB=1/4, PC=1/8, PD=1/8,

що можна інтерпретувати наступним чином: літери зустрічаються в середньому - А у половині випадків, чверть випадків припадає на літеру В, ще чверть випадків ділять порівну між собою літери С та D.

Тоді кількість інформації у повідомленні з 8 символів можливо розрахувати по формулі:

$I=-8\times(1/2\times\log_2 1/2+1/4\times\log_2 1/4+1/8\times\log_2 1/8+1/8\times\log_2 1/8)= 4+4+3+3=14$ (біт)

Аналіз формули Шеннона показує, що кількість інформації у двійковому поданні (у бітах або байтах) залежить від двох величин: кількості символів у повідомленні та частоти появи в повідомленнях того чі іншого символу з алфавіту, що використовується. Цей підхід не відображає наскільки корисна отримана інформація, але дозволяє порівняти відносну інформативність різних повідомлень та визначити витрати на передачу повідомлення.

II. Тезаурусний підхід (або семантична теорія інформації) був запропонований математиком Ю.А. Шрейдером, що народився в Україні. Цей підхід заснований на розгляді інформації як знань. Згідно з цим підходом кількість інформації, що отримується людиною з повідомлення, можна оцінити ступенем зміни його знань.

У словникової практиці тезаурусом прийнято називати одномовний асоціативний словник, в якому вказані різні смислові зв'язки між словами. Тезаурус, як і всякий довідник, відображає відомості, накопичені до певного моменту часу деяким суб’єктом (приймачем). Зокрема, він характеризує здатність цього суб’єкту сприймати ті чи інші повідомлення.

Тезаурус по Шрейдеру - це структуровані знання, представлені у вигляді понять і відносин між ними. Структура тезауруса ієрархічна (тобто має багаторівневу архітектуру). Поняття й відносини, групуючись, утворюють інші, більш складні поняття й відносини.

Знання окремої людини, організації, держави утворюють властиві їм тезауруси. Тезауруси організаційних структур утворюються тезаурусами складових їхніх елементів.

Так, тезаурус організації утворюють, насамперед, тезауруси співробітників, а також інших носіїв інформації, таких як документи, устаткування, продукція тощо. Для передачі знань потрібно, щоб тезауруси передавального та приймаючого елемента перетиналися, інакше – мали спільні знання. В іншому випадку власники тезаурусів не зрозуміють один одного.

Тезауруси фізичних і юридичних осіб є їхнім капіталом. Тому власники тезаурусів прагнуть зберегти й збільшити свій тезаурус. Збільшення тезауруса здійснюється за рахунок навчання, покупки ліцензій, запрошення кваліфікованих співробітників і навіть розкрадання інформації.

У суспільстві спостерігаються дві тенденції: розвиток тезаурусів окремих елементів (людей, організованих структур) і вирівнювання тезаурусів елементів суспільства. Вирівнювання тезаурусів відбувається як у результаті цілеспрямованої діяльності (наприклад, навчання), так і стихійно. Стихійне вирівнювання тезаурусів відбувається за рахунок випадкової передачі знань, включаючи незаконну передачу.

Цей підхід має великий потенціал для створення кібернетичних організмів – машин здатних подібно людині самостійно формувати нові знання, але складність реалізації цього підходу для практичної оцінки кількості інформації, та, відповідно, її цінності занадто велика.

III. Практичний підхід, не зважаючи на наведені вище недоліки, все ж таки базується на понятті «обсяг інформації». При цьому кількість інформації може вимірятися в кількості біт (байт), у кількості сторінок тексту, довжині магнітної стрічки з відео- або аудіозаписом тощо.

Однак очевидно, що одна сторінка будь-якого формату може містити більше або менше інформації, принаймні, з двох причин.

По-перше, різні люди можуть розмістити на сторінці різну кількість відомостей про один і той самий об'єкт, процес або явище матеріального світу. По-друге, різні люди можуть отримати з того самого тексту різну кількість корисної, зрозумілої для них інформації. Навіть та сама людина у різні роки життя одержує різну кількість інформації при читанні книги.

У результаті копіювання носія без зміни інформаційних параметрів кількість інформації не змінюється, а ціна в загальному випадку знижується. Прикладом копіювання без зміни інформаційних параметрів може слугувати копіювання тексту з використанням якісних копіювальних пристроїв.

Текст копії, за умов відсутності збоїв копіювального пристрою, буде містити точно таку ж інформацію, як і текст оригіналу. Але при копіюванні зображень вже складно уникнути спотворень. Їх кількість може бути тільки більшою або меншою.

У той же час, відповідно до законів ринку, чим більше товару з'являється, тем він дешевше. Цей закон повністю слушний і відносно копій інформації. Дію цього закону можна простежити на прикладі піратського поширення програмних продуктів, відеопродукції й т.п.

Інформація як об'єкт права власності

Особливості захисту інформації обумовлюються також різним статусом суб'єктів інформаційних відносин (особа, підприємство, суспільство, держава).

Різні суб'єкти інформаційних відносин стосовно певної інформації можуть виступати в якості (можливо одночасно):

- джерел (постачальників) інформації;
- користувачів (споживачів) інформації;
- власників (розпорядників) інформації;
- фізичних і юридичних осіб, про яких збирається інформація;
- власників систем збору й обробки інформації й учасників процесів обробки й передачі інформації.

Виникає складна система взаємостосунків між цими суб'єктами права власності.

Інформація як об'єкт права власності може бути скопійована за рахунок матеріального носія. Як наслідок, інформація як об'єкт права власності легко переміщається до іншого суб'єкта права власності без очевидного (помітного) порушення права власності на інформації.

Переміщення матеріального об'єкта до іншого суб'єкта права власності неминуче, і, як правило, спричиняє втрату цього об'єкта первинним суб'єктом права власності, тобто відбувається очевидне порушення його права власності.

Право власності включає три повноваження власника, що становлять зміст (елементи) права власності: право розпорядження, право володіння, права користування.

Але для необхідності розгляду інформації як предмета захисту інформації, необхідно розглянути особливості інформації як об'єкта права власності.

Суб'єкт права власності на інформацію може передати частину своїх прав (розпорядження), не втрачаючи їх, іншим суб'єктам, «хранителеві», тобто власникові матеріального носія інформації (володіння або користування) або користувачеві (користування й, може бути, володіння).

Для інформації право розпорядження має на увазі виключне право визначати, кому ця інформація може бути надана.

Право володіння має на увазі мати цю інформацію в незмінному виді. Право користування має на увазі право використовувати цю інформацію у своїх інтересах.

Таким чином, до інформації, крім суб'єкта права власності на цю інформацію, можуть мати доступ інші суб'єкти права власності, як законно, санкціоновано (суб'єкти права на елементи власності), так і незаконно, не санкціоновано. Таким чином, мета захисту інформації, полягає ще й у захисті прав власності на неї.

У рамках курсу переважно передбачається, що інформація використовується, зберігатися, передається й обробляється в різного роду комп’ютерних системах (КС).

Матеріальною основою існування інформації в КС, як правило, є електронні й електронно-механічні пристрої (підсистеми), а також машинні

носії. У якості машинних носіїв інформації можуть використовуватися папір, магнітні й оптичні носії, електронні схеми. Програмні засоби, що входять до складу КС самі по собі є інформаційними ресурсами.

Таким чином, необхідно захищати пристрої й підсистеми, а також машинні носії інформації. Тому, під поняттям об'єкт захисту інформації доцільно розуміти сукупність усіх носіїв інформації, що представляє собою комплекс фізичних, апаратних, програмних і документальних засобів.

У різних інформаційних системах користувачі інформаційних систем є обслуговуючим персоналом і можуть бути джерелами й носіями інформації.

Тому поняття об'єкта захисту трактується в більш широкому змісті. Під об'єктом захисту розуміється не тільки інформаційні ресурси, апаратні й програмні засоби, що обслуговує персонал і користувачі, але й приміщення, будинки, а також територія що безпосередньо оточує будівлі.

Поняття, сутність, цілі захисту інформації

У цьому розділі та наступних у випадках, коли необхідно приділити основну увагу технічним аспектам безпеки, у якості об’єкту захисту ми будемо переважно розглядати комп’ютерну систему, як сукупність апаратного та програмного забезпечення (технічної та програмної платформ), а також необхідної документації до неї.

Якщо організаційна складова безпеки є невід’ємною складовою, то в якості об’єкту захисту ми визначимо автоматизовану систему (АС), як організаційно-технічну систему, що додатково до складових комп’ютерної включає середовище користувачів системи.

Також залежно від особливостей функціонального призначення будемо розрізняти різновиди автоматизованих систем: інформаційні системи (ІС) та телекомунікаційні системи (ТС) або їх комбінацію – інформаційно-телекомунікаційні системи (ІТС).

В попередніх розділах було зазначено, що поняття захист інформації є невід'ємною складовою інформаційної безпеки.

Існує кілька визначень захисту інформації, обумовлених деякою неузгодженістю окремих нормативно-правових актів. Для розуміння процесів, методів і засобів захисту скористаємося наступним визначенням: під захистом інформації у вузькому змісті будемо розуміти сукупність дій та заходів, спрямованих на забезпечення безпеки інформації в контексті забезпечення конфіденційності, доступності й цілісності під час її збору, передачі, обробки й зберігання.

Безпека інформації – це властивість (стан) переданої, оброблюваної й збереженої інформації, що характеризує її ступінь захищеності від дестабілізуючого впливу зовнішнього середовища (людини й природи) і внутрішніх загроз, тобто її конфіденційність, доступність, і цілісність як стабільність до руйнуючих, імітуючих та спотворюючих впливів і перешкод.

Під захистом інформації, у більш широкому змісті, будемо розуміти комплекс організаційних, правових і технічних заходів щодо запобігання загрозам безпеці інформації й мінімізації негативних наслідків їх реалізації.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації джерел негативних впливів, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації. Мета й методи захисту інформації відображають її сутність.

Захист інформації забезпечується за наступними напрямами:

- ідентифікація загроз, що реалізується шляхом систематичного аналізу й контролю можливості появи реальних або потенційних загроз;

- виявлення загроз, суттю чого є визначення реальних загроз і конкретних протиправних дій;

- попередження загроз шляхом впровадження превентивних заходів для забезпечення інформаційної безпеки спрямованих на уникнення умов їх виникнення;

- нейтралізація загроз завдяки застосуванню корегуючих заходів та засобів;

- локалізація загроз передбачає виключення можливості поширення загроз за межі певної припустимої галузі;

- ліквідація загрози або конкретних протиправних дій;

- ліквідація наслідків загроз і протиправних дій і відновлення попереднього стану.

Ідентифікація має на меті проведення заходів щодо збору, накопичення й аналітичної обробки відомостей про можливу підготовку протиправних дій з боку кримінальних структур або конкурентів на ринку проведення й збуту товарів і продукції

Виявлення загроз – це дії по визначенню конкретних загроз і їх джерел, що приносять той або інший вид збитку інформаційним ресурсам, виявлення фактів розголошення інформації з обмеженим доступом (у т.ч. випадків несанкціонованого доступу до джерел комерційних секретів), порушення цілісності або доступності інформації.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими заходами й засобами, починаючи від створення клімату глибоко усвідомленого відношення співробітників до проблеми безпеки й захисту інформації до створення глибоко ешелонованої системи захисту фізичним, апаратними, програмними й криптографічними засобами.

Попередження загроз можливо й шляхом одержання інформації про протиправні акти, що готуються, запланованих розкраданнях, підготовчих діях і інших елементах злочинних діянь.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози й конкретних протиправних дій.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Наприклад, відновлення інформаційного ресурсу завдяки раніше зроблених його копій на резервних носіях інформації.

Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань та:

- запобігти витоку інформації з обмеженим доступом, виключити можливість несанкціонованого доступу до носіїв конфіденційної інформації;

- забезпечити цілісність та доступність інформації;

- підтвердити авторство визначеної інформації.

Враховуючи викладене, можливо зробити висновок, що захист інформації є діяльністю із застосуванням певної сукупності методів, засобів і заходів, які спрямовані на забезпечення інформаційної безпеки держави, суспільства й особистості у всіх областях їх життєво важливих інтересів.

Кожний вид інформації, що захищається, має свої особливості в області регламентації, організації й здійснення цього захисту.

Інформація, що захищається, може включати відомості, що становлять державну, комерційну, службову й інші охоронювані законом таємниці, як і будь-який інший вид інформації, вона необхідна для управлінської, науково-виробничої й іншої діяльності.

Найбільш загальними ознаками захисту/охорони будь-якого способу подання охоронюваної інформації є наступні:

- вимоги по захисту інформації й порядок її охорони/захисту визначає власник інформації (держава, підприємство, громадянин);

- безпосередньо захист інформації в інформаційно-телекомунікаційній системі на основі договору із власником інформації організує й проводить власник ІТС (тимчасовий розпорядник інформації) або уповноважені їм на те особи (юридичні або фізичні);

- захистом інформації її власник охороняє свої права на володіння й розпорядження інформацією, прагне захистити її від незаконного заволодіння й використання на шкоду його інтересам;

- захист інформації здійснюється шляхом проведення комплексу заходів щодо обмеження доступу до інформації, що захищається, і створенню умов, які виключають або суттєво ускладнюють несанкціонований, нелегальний доступ до інформації, що захищається, і її носіям.

Загалом, захист інформації – це комплекс заходів, проведених власником інформації, по огородженню своїх прав на володіння й розпорядження інформацією, створенню умов, що обмежують її поширення, що й виключають або істотно ускладнюють незаконний доступ до інформації з обмеженим доступом і її носіям.

У зв'язку з автоматизованою обробкою даних перед захистом інформації ставляться більш широкі завдання, ніж недопущення несанкціонованого доступу до неї. Це обумовлено рядом обставин, і в першу чергу тим, що в комп'ютерних системах може відбуватися не тільки витік інформації, але і її руйнування, викривлення, підробка, блокування й інші втручання в інформаційні ресурси та інформаційні процеси.

Отже, захист інформації повинен передбачати також забезпечення безпеки засобів інформації, у яких накопичується, обробляється й зберігається інформація, що захищається.

Таким чином, захист інформації – це діяльність власника інформації або уповноважених їм осіб по:

- забезпеченню своїх прав на володіння, розпорядження й управління інформацією, що захищається;

- запобіганню витоку й втрати інформації;

- збереженню повноти, вірогідності, цілісності інформації, що захищається, її масивів і програм обробки;

- збереженню конфіденційності або таємності інформації, що захищається, відповідно до правил, установлених законодавчими і іншими нормативними актами.

Основними цілями захисту інформації є унеможливлення або мінімізація ризиків реалізації загроз безпеки особистості, суспільства, держави внаслідок:

- витоку, розкрадання, втрати, викривлення, модифікації, підробки інформації;

- несанкціонованих дій по знищенню, викривленню, копіюванню, блокуванню інформації у комп'ютерних системах;

- незаконного втручання в інформаційні ресурси й інформаційні системи;

- порушення правового режиму документованої інформації як об'єкта власності;

- порушення конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, наявних в інформаційних системах;

- витоку документованої інформації, що містить державну таємницю відповідно до законодавства;

- порушення прав суб'єктів інформаційних процесів при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їх забезпечення.

З аналізу загроз безпеки інформації, цілей і завдань її захисту випливає, що досягти необхідного рівня захищеності можна тільки за рахунок певних принципів захисту інформації до яких належіть комплексне використання існуючих методів і засобів захисту, безперервну реалізацію заходів із захисту інформації, необхідність та достатність комплексу засобів та заходів, адекватність витрат на захист вартості можливої шкоди внаслідок реалізації загроз.

Головним принципом захисту інформації є забезпечення комплексного підходу, завдяки якому досягається ефективний захист за умов певних витрат на його реалізацію. Саме цей принцип має бути покладений в основу розробки як концепції захисту інформації, так і конкретних систем захисту.

Мета захисту інформації на об'єктах захисту може бути досягнута за умов проведення комплексу робіт з наступних напрямків:

- визначенню охоронюваних відомостей;

- виявленню й усуненню (ослабленню) демаскуючих ознак, що розкривають охоронювані відомості;

- оцінці можливостей і ступеню небезпеки використання технічних засобів розвідки;

- виявленню можливих технічних каналів витоку інформації;

- аналізу можливостей і небезпеки несанкціонованого доступу до інформаційних об'єктів;

- аналізу небезпеки знищення або викривлення інформації за допомогою програмно-технічних впливів на об'єкти захисту;

- розробці й реалізації організаційних, технічних, програмних і інших засобів і методів захисту інформації від усіх можливих загроз;

- створенню комплексної системи захисту;

- організації й проведенню контролю стану й ефективності системи захисту інформації;

- забезпеченню стійкого керування процесом функціонування системи захисту інформації.

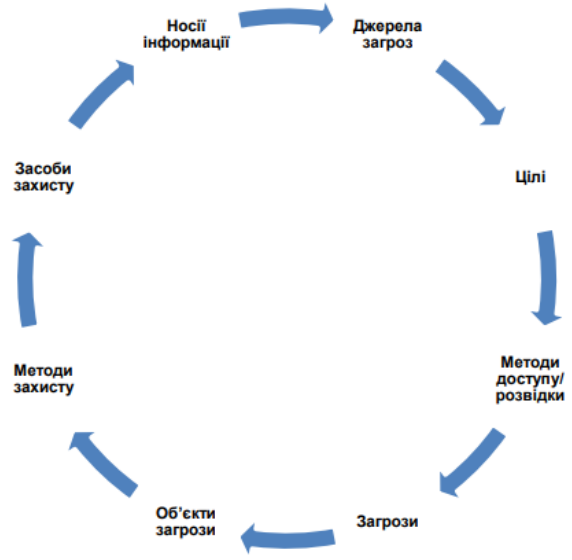
Процес захисту інформації повинен здійснюватися безупинно на всіх етапах. Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, впровадження надійних механізмів захисту й забезпечення їх сталого функціонування й високої ефективності, провадження відповідних робіт тільки фахівцями високої кваліфікації в області захисту інформації.

Загальна модель інформаційної безпеки

На відміну від загроз випадкового характеру, що обумовлені помилками персоналу, який обслуговує автоматизовані системи, природними катаклізмами та збоями техніки, реалізація навмисних загроз порушником відповідає процесній моделі діяльності с чітко визначеними цілями та завданнями.

В цьому випадку надійна система інформаційної (кібернетичної) безпеки утворює перешкоду на шляху досягнення атакуючою стороною певних цілей. Остання корегує власні дії та може вживати необхідних заходів щодо уточнення тактики дій (посилення тиску, вибір більш ефективних засобів тощо), а це, в свою чергу, вимагає від суб’єктів системи захисту реалізації заходів щодо корегування методи та/або зміни засоби захисту інформації.

Таким чином, ситуація щодо атак на інформаційні ресурси та забезпечення їх безпеки має циклічний характер, саме така, циклічна модель забезпечення безпеки інформації від навмисних загроз зображена на рис. 1. Точніше, відповідно до принципів діалектики, модель повинна мати спіральний вигляд, оскільки «кожен новий віток» протистояння «атака – захист» відбувається на якісно новому рівні.



У той же час для розуміння проблеми достатньо «двомірної» моделі. Вона включає наступні елементи:

- носії інформації (особи, що обізнані з таємницею, документальні матеріали, машинні носії, фізичні поля), що об’єктом зацікавленості відповідного суб’єкту (конкурента, зловмисника або спецслужби);
- джерела загроз інформації (конкуренти, зловмисники, спеціальні служби);
- цілі порушників (здобуття цінної інформації науково-технічного характеру, інформації у сфері безпеки та оборони, нанесення збитків, отримання переваг, корисні мотиви тощо);
- методи доступу (агентурні, технічні);
- загрози інформації (конфіденційності, цілісності, доступності);
- об’єкти загроз (відомості економічного, науково-технічного, оборонного характеру тощо);
- методи захисту (правові, організаційні, інженерно-технічні, а також технічний, криптографічний та стеганографічний захист);
- засоби захисту (технічні, апаратні та програмні в комп’ютерних системах, і, додатково, організаційні в автоматизованих системах).

В рамках вказаної моделі кожна попередня сутність впливає на стан/поведінку (вибір варіанту) наступної сутності.

Забезпечення інформаційної безпеки (у вузькому змісті безпеки інформації) – це комплексна проблема, розв'язання якої на практиці вимагає ефективного сполучення нормативно-правових заходів (законодавчий рівень), організаційних заходів, інженерно-технічних методів і засобів, блокування та нейтралізації технічних каналів витоку інформації (адміністративний і процедурний рівень), методів і засобів криптографічного та технічного і захисту (програмно-технічний рівень).

Законодавчий рівень (рис. 2) є найважливішим для забезпечення інформаційної безпеки.

Розробка й прийняття правових норм покликані врегулювати питання використання інформаційної структури й телекомунікацій, доступу до інформації, захисту інформації від несанкціонованого доступу й витоку по технічних каналах, захисту громадян, суспільства й держави від неправдивої інформації, захисту інформаційно-телекомунікаційних систем від неправомірних дій, забезпечення інформаційних аспектів техногенної безпеки тощо.

У випадку формування законодавства в сфері інформаційних ресурсів і комунікацій у самостійну галузь права – інформаційне право – законодавство в сфері забезпечення інформаційної безпеки буде виступати як його підгалузь, а при кодифікації у вигляді Інформаційного кодексу стане його складовою частиною.

Прийнято виділяти два напрямки формування законодавства. До першого належать заходи, спрямовані на створення й підтримку в суспільстві негативного відношення до порушень і порушників інформаційної безпеки.

В українському законодавстві сюди можна віднести відповідні глави Кримінального кодексу України.

До другого напрямку можна віднести законодавчі акти й нормативні документи, що сприяють підвищенню освіченості суспільства в області інформаційної безпеки, визначають певний порядок здійснення діяльності в області технічного й криптографічного захисту інформації, розробки засобів захисту, встановлюють критерії якості виконання робіт та надання послуг тощо.

Основу заходів адміністративного рівня, тобто заходів, що реалізуються керівництвом організації, становить політика безпеки.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

Політика безпеки визначає стратегію організації в галузі інформаційної безпеки, а також ресурси, які керівництво вважає за можливе виділити для реалізації її завдань.

На підставі політики безпеки будується програма безпеки, яка реалізується на процедурному й програмно-технічному рівнях.

Процедурний рівень передбачає заходи безпеки, що реалізуються персоналом організації.

Можна виділити наступні групи процедурних заходів:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відбудовних робіт.

Управління персоналом полягає у виконанні наступних умов. По-перше, для кожної посади повинні існувати кваліфікаційні вимоги по ІБ. По-друге, у посадові інструкції повинні входити розділи, що стосуються інформаційної безпеки. По-третє, кожного співробітника потрібно навчити заходам безпеки теоретично й на практиці.

Заходи фізичного захисту містять у собі захист від витоку інформації по технічних каналах, інженерні способи захисту тощо.

Планування відбудовних робіт передбачає:

- злагодженість дій персоналу під час і після аварії;
- наявність заздалегідь підготовлених резервних виробничих майданчиків;
- офіційно затверджену схему перенесення на резервний майданчик основних інформаційних ресурсів;
- схему повернення до нормального режиму роботи.

Підтримка працездатності містить у собі створення інфраструктури, що включає в себе як технічні, так і процедурні регулятори й здатної забезпечити наперед заданий рівень працездатності на всьому протязі життєвого циклу інформаційної системи.

Реагування на порушення режиму безпеки може бути регламентоване в рамках окремо взятої організації. У поточний час, переважно здійснюється моніторинг комп'ютерних злочинів у національному масштабі й по окремих статтях законодавства «підвідомчих» Службі безпеки України або Міністерству внутрішніх справ України збуджуються кримінальні справи у випадку наявності складу злочину.

Основу програмно-технічного рівня становлять наступні механізми безпеки:

- захист від несанкціонованого доступу у комп’ютерних системах, що включає ідентифікацію й автентифікацію суб’єктів (користувачів) та об’єктів (ресурсів), управління доступом, протоколювання дій та подій, аудит та тестування системи безпеки;
- криптографічний захист інформації, який реалізується, зокрема, шляхом шифрування інформації, формування та перевірки електронного цифрового підпису, реалізації захищених протоколів автентифікації;
- виявлення та блокування технічних каналів витоку інформації або впливу на неї;
- захист від впливу шкідливих кодів (антивірусний захист);
- убезпечення інформаційних систем від атак що спрямовані на відмову в обслуговуванні;
- захист від атак які націлені на перехоплення управління в автоматизованих або автоматичних (працюючих без втручання операторів) системах.

Важливо ефективно управляти інформаційною системою в цілому й механізмами безпеки особливо. Згадані заходи безпеки повинні спиратися на загальноприйняті стандарти, бути стійкими до мережних загроз, враховувати специфіку окремих сервісів, а також властивості інформації як предмета захисту.

Різноманіття нормативних документів презентовано міжнародними, національними, галузевими нормативними документами й відповідними нормативними документами організацій, підприємств і фірм.

Велику роботу в цьому напрямку проводять Інститут інженерів електротехніки та електроніки – IIEE (IEEE), Міжнародна організація по стандартизації – МОС (ISO), Міжнародна електротехнічна комісія – МЕК (IEC), Міжнародний союз електрозв'язку – МСЕ (ITU).

IIEE є професійним об’єднанням, що працює у галузі нормування та досліджень в електротехніці та комп’ютерних науках, інженерії та суміжних науках. Його діяльність щодо кібернетичної безпеки реалізується шляхом розробки технічних стандартів в рамках Асоціації стандартів IIEE. Серед найбільш відомих здобутків IIEE спільна з Національним інститутом стандартів і технологій (NIST, США) у розробці серії стандартів NERC CIP для систем управління кібернетичними активами електроенергетичних компаній.

МЕК об’єднує представників національних комітетів з стандартизації 70 країн, до складу яких в свою чергу входять спеціалісти з державного та приватного секторів. МЕК спільно з МОС через Об’єднаний технічний комітет (JTC) розробили серію стандартів ISO/IEC27001 що регулює питання створення системи управління інформаційною безпекою, та загально відомий стандарт якості ISO/IEC9001

МОС є неурядовою організацією, що розробляє та видає міжнародні стандарти, в її роботі беруть участь представники понад 160 країн світу. Стандарти МОС (ISO) використовуються в багатьох галузях, у тому числі, в інформаційних та телекомунікаційних технологіях, деякі криптографічні алгоритми шифрування та цифрового підпису визначені як стандарти ISO.

МСЕ (ITU-T) працює на правах агентства Організації об’єднаних націй, його членами є понад 190 країн світу. До МСЕ компетенції належать розроблення технічних стандартів, розподіл радіочастот та деякі інші питання. Генеральним секретаріатом МСЕ підготовлено Глобальну програму кібернетичної безпеки (GCA) що спрямована на формування єдиного скоординованого міжнародного підходу до кібернетичної безпеки. Ця Програма стосується п’ятьох аспектів, а саме: 1) законодавчих мір, 2) технічних та процедурних заходів, 3) організаційних структур, 4) створення потенціалу та 5) міжнародного співробітництва. Серед здобутків вказаної організації слід відмітити стандарт що встановлює формати сертифікатів відкритих ключів X.509.

Слід зазначити, провідні національні організації із стандартизації також додають значних зусиль щодо розробки та впровадження кращих нормативів у сфері захисту інформації. Зокрема, розроблення технічних стандартів в сфері інформаційної безпеки, включаючи аспекти криптографічного захисту інформації та комп’ютерної безпеки, здійснюють:

- Американський національний інститут стандартів (англ. American National Standards Institute, ANSI) — об’єднання американських промислових і ділових груп, що розробляє стандарти, зокрема, в комунікаційній сфері. ANSI в організаціях ISO та IEC представляє США;

- Національний інститут стандартів і технологій (англ. The National Institute of Standards and Technology, NIST) підрозділ Управління з технологій одного з агентств Міністерства торгівлі США,

- Британський інститут стандартів (British Standards Institution – BSI),

- Німецький інститут стандартизації (Deutsches Institut für Normung e.V. — DIN) тощо.

В Україні технічне регулювання в сфері криптографічного та технічного захисту інформації змінює Держстандарт України спільно з Держспецзв'язку України. Зокрема, в галузі технічного захисту інформації в Україні розроблені та діють наступні державні стандарти:

- ДСТУ 3396.0-96. "Захист інформації. Технічний захист інформації. Основні положення". Цей стандарт встановлює об'єкт, мету, організаційні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) і державі, а також категорії нормативних документів системи ТЗІ.

- ДСТУ 3396.1-96. "Захист інформації. Технічний захист інформації. Порядок проведення робіт". Стандарт встановлює вимоги до порядку проведення робіт з технічного захисту інформації.

- ДСТУ 3396.2-96. "Захист інформації. Технічний захист інформації. Терміни й визначення". Даний стандарт встановлює терміни й визначення понять у сфері ТЗІ.

Серед міжнародних стандартів в галузі інформаційної безпеки слід відмітити загально відомий британський – BS 7799 та розроблений на його основі стандарт ISO/IEC27001:2005 (поточна редакція ISO/IEC27001:2013), розмова про які буде у наступних розділах.

Нормативне регулювання порядку проведення робіт зі стандартизації й сертифікації в області захисту інформації враховує два аспекти: формальний – визначення критеріїв, яким повинні відповідати захищені інформаційні технології й практичний – визначення конкретного комплексу заходів безпеки стосовно розглянутої інформаційної технології.

Основними критеріями працездатності концепцій і стандартів у галузі інформаційної безпеки вважаються наступні:

- універсальність – характеристика стандарту, що залежить від множини типів обчислювальним систем, на які він орієнтований;

- гнучкість – можливість застосування стандарту до інформаційних технологій, що постійно розвиваються;

- гарантуємість – кількість і якість передбачених стандартом методів і засобів підтвердження надійності результатів кваліфікаційного аналізу;

- реалізуємість – можливість адекватної реалізації на практиці;

- актуальність – вимоги й критерії стандарту повинні відповідати множині, загроз безпеці, що постійно розвивається.

Виходячи з подібних критеріїв оцінки, найбільш працездатним зі створених уже документів уважають «Єдині загальні критерії оцінки безпеки інформаційних технологій», що представляє собою результат спільної роботи Міжнародної організації по стандартизації, Національного інституту стандартів і технологій США, організацій Великобританії, Канади, Німеччини, Франції й Нідерландів.

ТЕМА 3. Джерела загроз інформації

Сутність потенційних та реальних загроз інформації

Одним з найважливіших аспектів проблеми створення ефективного гарантованого захисту інформації є визначення, аналіз і класифікація можливих загроз безпеці інформації.

Під загрозою безпеці будемо розуміти потенційно можливу подію, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації.

Загрози можна класифікувати по відношенню джерела загрози до об'єкта захисту (зовнішні й внутрішні), по виду джерела загроз (фізичні, логічні, комунікаційні, людські), по ступеню злого наміру (випадкові й навмисні) і т.д.

Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника є основою для проведення аналізу ризику й формулювання вимог до системи захисту інформації.

Усю множину загроз можна розділити на два класи:

- випадкові або ненавмисні;
- навмисні.

Загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають випадковими або ненавмисними.

Реалізація загроз цього класу приводить до найбільших втрат інформації (за статистичним даними – до 80% збитків від усіх можливих загроз). При цьому можуть відбуватися знищення, порушення цілісності й доступності інформації. Рідше порушується конфіденційність інформації, однак при цьому створюються передумови для протиправного впливу на інформацію.

Стихійні лиха й аварії чреваті найбільш руйнівними наслідками для матеріальних джерел зберігання інформації, тому що останні зазнають фізичного руйнування, інформація втрачається або доступ до неї стає неможливий.

Збої й відмови складних систем неминучі. У результаті порушується працездатність технічних засобів, знищуються й спотворюються дані й програми. Порушення роботи окремих вузлів і пристроїв можуть також призвести до порушення конфіденційності інформації. Наприклад, збої й відмови засобів видачі інформації можуть призвести до несанкціонованого доступу до інформації шляхом несанкціонованої її видачі в канал зв'язку, на друкувальний пристрій.

Помилки при розробці комп’ютерної системи, алгоритмічні й програмні помилки приводять до наслідків, аналогічних наслідкам збоїв і відмов технічних засобів. Крім того, такі помилки можуть бути використані зловмисниками для впливу на ресурси системи. Особливу небезпеку становлять помилки в операційних системах і в програмних засобах захисту інформації.

Згідно даним Національного інституту стандартів і технологій США, 65% випадків порушення безпеки інформації відбувається в результаті помилок користувачів і обслуговуючого персоналу. Некомпетентне, недбале або неуважне виконання співробітниками функціональних обов'язків призводять до

знищення, порушення цілісності й конфіденційності інформації, а також компрометації механізмів захисту.

Характеризуючи загрози інформації, не пов'язані з навмисними діями, у цілому, слід зазначити, що механізм їх реалізації вивчений досить добре, накопичений значний досвід протидії цим загрозам. Сучасна технологія розробки технічних і програмних засобів, ефективна система експлуатації комп'ютерних систем, що включає обов'язкове резервування інформації, дозволяють значно знизити втрати від реалізації загроз цього класу.

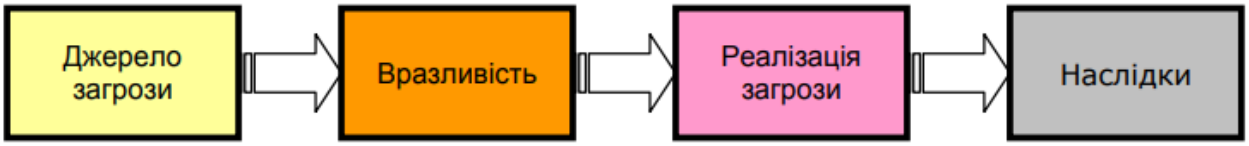
Другий клас загроз безпеки інформації становлять навмисно створювані загрози.

Даний клас загроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими загрозами. Загрози цього класу залежно від методів реалізації, їхньої фізичної сутності можуть бути розподілені по п'ятьом групах:

- традиційне шпигунство (із залученням секретних агентів), інакше – агентурна розвідка;
- тероризм і диверсії;
- несанкціонований доступ до інформації в комп'ютерних системах;
- технічна розвідка, що включає візуальну, акустичну та радіоелектронну розвідки;
- кібернетичні атаки на комп'ютерні системи що спрямовані на блокування інформаційних ресурсів, перехоплення управління автоматизованими системами, модифікацію або руйнування їх інформаційних структур, в т.ч. із застосовуванням шкідницьких програм.

Джерела виникнення загроз та шляхи їх реалізаці

Організація забезпечення захисту інформації повинна передбачати обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву (вразливості) і, як наслідок, визначення актуальних загроз БП. Виходячи з цього, моделювання й класифікацію джерел загроз та їх проявів, доцільно проводити на основі аналізу взаємодії логічного ланцюга.



Логічний ланцюг взаємодії джерела загроз та вразливості

У якості джерел небажаного впливу на інформаційні ресурси як і раніше актуальні методи й засоби шпигунства й диверсій, які використовувалися й використовуються для добування або знищення інформації на об'єктах, що не мають комп'ютерних систем. Ці методи також дієві й ефективні в умовах застосування комп'ютерній систем. Найчастіше вони використовуються для одержання відомостей про систему захисту з метою проникнення в інформаційну систему, а також для розкрадання й знищення інформаційних ресурсів.

Терор та диверсії реалізуються не тільки шляхом підпалів, вибухів, захоплення заручників, транспортних засобів та високотехнологічних

виробництв, а й завдяки застосуванню методів спрямованого надпотужного електромагнітного випромінюванню.

Для деяких об'єктів інформаційних систем і зберігання інформації існує загроза збройного нападу терористичних (диверсійних) груп. При цьому можуть бути застосовані засоби вогневої поразки.

Серед можливих методів шпигунства слід відмітити:

- розкрадання документів і машинних носіїв інформації, програм і атрибутів системи захисту;
- підкуп і шантаж співробітників;
- збір і аналіз відходів машинних носіїв інформації;
- підслуховування;
- візуальне спостереження;

Шпигунство (розкрадання документів та інформації, вербування співробітників об'єктів автоматизованої системи) може здійснюватися завдяки безпосередньому доступу на об'єкт або без цього.

Зловмисниками, що мають доступ на об'єкт, можуть використовуватися мініатюрні засоби фотографування; відео- і аудіозапису.

Для аудіо- і відеоконтролю приміщень і при відсутності в них зловмисника застовуються закладні пристрої або «жучки». Для об'єктів інформаційних систем найбільш імовірними є закладні пристрої, що забезпечують прослуховування приміщень.

Вітчизняне законодавство класифікує заставні пристрої як спеціальні технічні засоби негласного знімання інформації.

Такі засоби діляться на провідні й випромінюючі. Провідні закладні пристрої вимагають значного часу на установку й мають певні демаскуючі ознаки їх впровадження.

Випромінюючі «закладки» («радіозакладки») швидко встановлюються, можуть працювати тривалий час автономно завдяки внутрішнім батарейкам але вони також мають демаскуючу ознаку – випромінювання в радіо або оптичному діапазоні. «Радіозакладки» можуть використовувати в якості джерела живлення мережі електричних або акустичних сигналів (телефонний та гучномовний зв'язок). Вказані мережі можуть бути одночасно джерелом інформації, що перехоплюється.

Велике поширення дістали акустичні «радіозакладки». Вони сприймають акустичні хвилі, перетворюють їх в електричний сигнал, що передається у вигляді радіосигналу на дальність до 8 км.

Із застосовуваних на практиці «радіозакладок» переважна більшість розраховані на роботу в діапазоні відстаней 50…800 метрів.

Для підслуховування зловмисникові не обов'язково проникати на об'єкт. Сучасні технічні засоби дозволяють підслухувати розмови з відстані декількох сотень метрів. У міських умовах дальність ефективної дії цих засобів може скорочуватися до десятків метрів залежно від рівня шуму навколишнього середовища - фонового шуму.

За допомогою спеціальних пристроїв, закріплених на шибках, їх механічні коливання скла, що обумовлені тиском акустичних хвиль у

приміщенні, реєструються та перетворюються в електричний сигнал. Передавання його на відстань здійснюється по радіоканалу.

Існують засоби підслуховування, що дозволяють з відстані до 1 км фіксувати розмови в приміщенні із закритими вікнами. Принцип дії таких пристроїв заснований на використанні відбитого променю лазера від скла вікна, яке коливається під впливом звукових коливань.

Розмови в сусідніх приміщеннях, а також за стінами будинків можуть контролюватися за допомогою стетоскопних мікрофонів, що за принципом дії нагадують відповідні медичні прилади. Стетоскопи перетворюють акустичні коливання в електричні з наступним зворотнім перетворенням в звукові хвилі. За допомогою таких засобів можливе прослуховування розмов при товщині стін до 50…100 см.

Поза приміщеннями, за звичай, підслуховування ведеться за допомогою надчуттєвих спрямованих мікрофонів. Реальна відстань підслуховування за допомогою спрямованих мікрофонів становить 50…100 метрів.

Оскільки під час розмов та звукової трансляції в такт із звуковим хвилями відбувається інших елементів конструкції, тому знімання відповідної інформації може також здійснюватися з металоконструкцій будинків, труб водопостачання, опалення, вентиляції.

Аудіоінформація може бути отримана також шляхом високочастотного нав'язування. Суть цього методу полягає у впливі високочастотним електромагнітним полем або електричними сигналами на елементи, здатні змінювати (модулювати) ці поля, електричними або акустичними сигналами з мовною інформацією. Модулювання – це електротехнічний термін, що означає зміну деякої характеристики сигналу (наприклад, його розмаху – амплітуди) в такт зі корисних сигналом (у т.ч. – звуковими хвилями).

У якості таких елементів можуть використовуватися різні порожнини з електропровідною поверхнею (сейфи, металеві шафи), що фактично являють собою великий високочастотний контур - своєрідну котушку індуктивності з розподіленими параметрами, які змінюються під дією акустичних хвиль.

При збігу частоти такого контуру із частотою високочастотного нав'язування й при наявності впливу акустичних хвиль на поверхню порожнини контур перевипромінює й модулює зовнішнє поле - високочастотний електричний сигнал.

Нерідко цей метод прослуховування реалізується за допомогою телефонної лінії. При цьому в якості модулюючого елемента використовується стаціонарний телефонний апарат, на який по телефонних проводах подається високочастотний електричний сигнал. Нелінійні елементи телефонного апарата під впливом мовного сигналу модулюють високочастотний сигнал. Модульований високочастотний сигнал відновлюється (демодулюється) у приймачі зловмисника.

Одним з можливих каналів витоку звукової інформації може бути прослуховування переговорів, що ведуться за допомогою засобів зв'язку. За допомогою спеціальних засобів радіоелектронної розвідки можуть контролюватися як радіоканали, так і провідні канали зв'язку. Нерідко,

прослуховування переговорів по провідних і радіоканалах не вимагає коштовного обладнання й високої кваліфікації зловмисника.

Дистанційна відеорозвідка для одержання інформації в автоматизованих системах неефективна й носить, як правило, допоміжний характер. Переважно, вона використовується для отримання секретних параметрів системи захисту інформації, включаючи ключі та паролі доступу.

Відеорозвідка також використовується для виявлення і розташування елементів системи захисту на об’єкті інформаційної діяльності та особливостей їх роботи. В комп’ютерних системах інформація реально може бути отримана при відображенні на екранах моніторів та табло, якщо є прозорі вікна й згадані засоби розміщені без урахування необхідності протидії такій загрозі.

Відеорозвідка може вестися з використанням технічних засобів, таких як оптичні прилади, фото-, кіно- і телеапаратура. Багато із цих засобів допускають запам'ятовування відеоінформації, а також її передачу на певні відстані.

Термін несанкціонований доступ до інформації (НСД) визначений як доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів комп’ютерних систем.

Під правилами розмежування доступу розуміється сукупність положень, що регламентують права доступу осіб або процесів (суб'єктів доступу) до одиниць інформації (об'єктів доступу).

Право доступу до ресурсів автоматизованих систем визначається керівництвом для кожного співробітника відповідно до його функціональних обов'язків.

Процеси ініціюються в інформаційних системах в інтересах певних задач та осіб, тому й на них накладаються обмеження щодо доступу до ресурсів.

Виконання встановлених правил розмежування доступу в інформаційних системах реалізується за рахунок створення системи розмежування доступу (СРД).

Несанкціонований доступ до інформації з використанням штатних апаратних і програмних засобів відбувається в наступних випадках:

- відсутність системи розмежування доступу, помилки в її елементах зроблені під час розробки, збій або відмова в її функціонуванні;
- помилки користувачів автоматизованих систем або адміністраторів безпеки;
- фальсифікація повноважень або навмисне блокування роботи СРД.

Якщо СРД відсутня, то зловмисник, що має навички роботи в інформаційній системі, може одержати без обмежень доступ до будь-якої інформації.

У результаті збоїв або відмов засобів системи, а також помилкових дій обслуговуючого персоналу й користувачів можливі стани системи, при яких спрощується НСД. Зловмисник може виявити помилки в СРД і використовувати їх для НСД.

Фальсифікація повноважень є одним з найбільш імовірних шляхів (каналів) НСД. Для цього зловмисником можуть використовуватися певні обманні дії, наприклад, створення підроблені інформаційні ресурси, під час

помилкового звернення до яких відбувається крадіжка особистої ідентифікаційної інформації.

Процес обробки й передачі інформації за допомогою електронних засобів, включаючи комп'ютерну техніку, супроводжується випромінюванням в навколишній простір електромагнітних хвиль і наведенням електричних сигналів у лініях зв'язку, сигналізації, заземленні й інших провідниках. Вони одержали назви побічних електромагнітних випромінювань і наведень (ПЕМВН).

За допомогою спеціального обладнання такі сигнали на відстані до декількох кілометрів можуть бути перехоплені приймачем зловмисника, виділені на фоні інших, підсилені, записувані в запам'ятовувальних пристроях та використані для здобування необхідної інформації.

Зокрема, досить великий рівень електромагнітного випромінювання притаманний працюючим пристроям відображення інформації (моніторам) на електронно-променевих трубках. Зображення на екрані такого монітору може переглядатися навіть за допомогою звичайного телевізійного приймача, що доповнений нескладним пристроєм, основною функцією якого є забезпечення синхронізація сигналів.

Дальність задовільного приймання таких сигналів при використанні дипольної (двопроменевої) антени сягає 50 метрів. Використання спрямованої антени приймача дозволяє збільшити зону впевненого прийому до 1 км.

Випромінювання неекранованих електричних кабелів залежно напругі струму, що протікає в них, можливо зареєструвати на відстані до 300 метрів.

Для здобування інформації зловмисник може використовувати також «просочування» інформаційних сигналів у ланцюги електроживлення технічних засобів.

«Просочування» інформаційних сигналів у ланцюги електроживлення можливо при наявності магнітного зв'язку між вихідним трансформатором підсилювача й трансформатором випрямляючого пристрою.

«Просочування» також можливе за рахунок спадання напруги на внутрішньому опорі джерела живлення при проходженні струмів посилюваних інформаційних сигналів. Якщо загасання у фільтрі випрямного пристрою недостатньо, то інформаційні сигнали можуть бути виявлені в ланцюзі живлення.

Інформаційний сигнал може бути виділений у ланцюзі живлення за рахунок залежності рівня загального споживаного струму від значень струму в різних, переважно, кінцевих каскадах підсилювачів інформаційних (у т.ч. звукових) сигналів.

Слід звернути увагу на те, що електромагнітні випромінювання можуть бути використані зловмисниками не тільки для одержання інформації, але й для її знищення.

Зокрема, потужні електромагнітні імпульси здатні знищити інформацію на магнітних носіях. Потужні електромагнітні й надвисокочастотні випромінювання можуть вивести з ладу електронні блоки системи. Причому

для знищення інформації на магнітних носіях з відстані декількох десятків метрів може бути використаний пристрій, що розміщується в невеликому кейсі.

Велику загрозу безпеки інформації в автоматизованій системі представляє несанкціонована модифікація алгоритмічної, програмної й технічної структур системи.

Несанкціонована модифікація структур може здійснюватися на будьякому життєвому циклі інформаційної системи.

Несанкціонована зміна структури системи на етапах розробки й модернізації одержала назву «закладка». Як правило, «закладка» у процесі розробки може бути цілеспрямовано впроваджена у спеціалізовану систему, яка призначена для експлуатації в державних органах та установах, де обробляється певна критична інформація, також мали місце випадки впровадження закладок в потужних фінансових установах.

Відомі випадки поставок подібного роду засобів з «закладками» потенційно небезпечним державам. Найбільш відомою ситуацією, в який була застосована подібна «закладка», є заходи з дистанційного відключення системи управління протиповітряної оборони іракського агресора під час проведення військової операції «Буря в пустелі».

«Закладки», впроваджені на етапі розробки, складно виявити через високу кваліфікацію їх розроблювачів і складності побудови сучасних інформаційних систем.

Алгоритмічні, програмні й апаратні «закладки» можуть бути використані або для безпосереднього шкідливого впливу на інформаційну систему, або для забезпечення НСД у систему.

Шкідливі впливи «закладок» на систему активуються при одержанні відповідної команди ззовні (в основному це характерно для апаратних «закладок») і при настанні певних подій у системі. Такими подіями можуть бути, перехід на певний режим роботи (наприклад, бойовий режим системи керування зброєю), настання встановленої дати, напрацювання певного часу тощо).

Програмні й апаратні «закладки», що застосовуються для здійснення неконтрольованого входу в програми, використання привілейованих режимів роботи (наприклад, режимів операційної системи), обходу засобів захисту інформації, одержали назву люків (англ. back door).

Одним з основних джерел загроз безпеки інформації в комп'ютерних системах є спеціально створені програми, що одержали загальну назву шкідливі кодів (програм). Залежно від механізму дії шкідливі програми поділяють на чотири класи:

- «логічні бомби»;
- «хробаки»;
- «троянські коні»;
- «комп'ютерні віруси».

«Логічні бомби» - це програми або їх частини, що постійно перебувають у комп'ютерних системах і виконуються тільки при певних умовах. Прикладами

таких умов можуть бути: настання заданої дати, перехід системи в певний режим роботи, настання деяких подій, установлене число разів тощо.

«Хробаками» називаються програми, які виконуються щораз при завантаженні системи, мають здатність переміщатися в обчислювальних системах або мережі й саме відтворювати копії. Лавиноподібне розмноження таких кодів призводить до перевантаження каналів зв'язку, пам'яті й, в остаточному підсумку, до блокування системи.

«Троянські коні» - це програми, що створені шляхом зміни або додавання кодів або команд у користувацькі програми. При наступному виконанні користувацьких програм поряд із заданими функціями виконуються несанкціоновані, змінені або якісь нові функції.

«Комп'ютерні віруси». Це невеликі програми, які після впровадження в комп'ютер самостійно поширюються шляхом створення своїх копій, а при виконанні певних умов впливають на інформаційні системи. Оскільки вірусам притаманні властивості всіх класів шкідливих програм, то останнім часом будь-які шкідливі програми часто називають вірусами.

Класифікація загроз інформації в комп’ютерній системі

Загроза безпеки інформації - це дія, спрямована проти об'єкта захисту, що проявляється в небезпеці викривлень і втрат інформації.

Джерела загроз безпеки можуть перебувати як усередині організації - внутрішні джерела, так і поза нею - зовнішні джерела.

Виходячи із проведеного аналізу, усі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

I. Загрози, що обумовлені діями суб'єктів - антропогенні загрози;

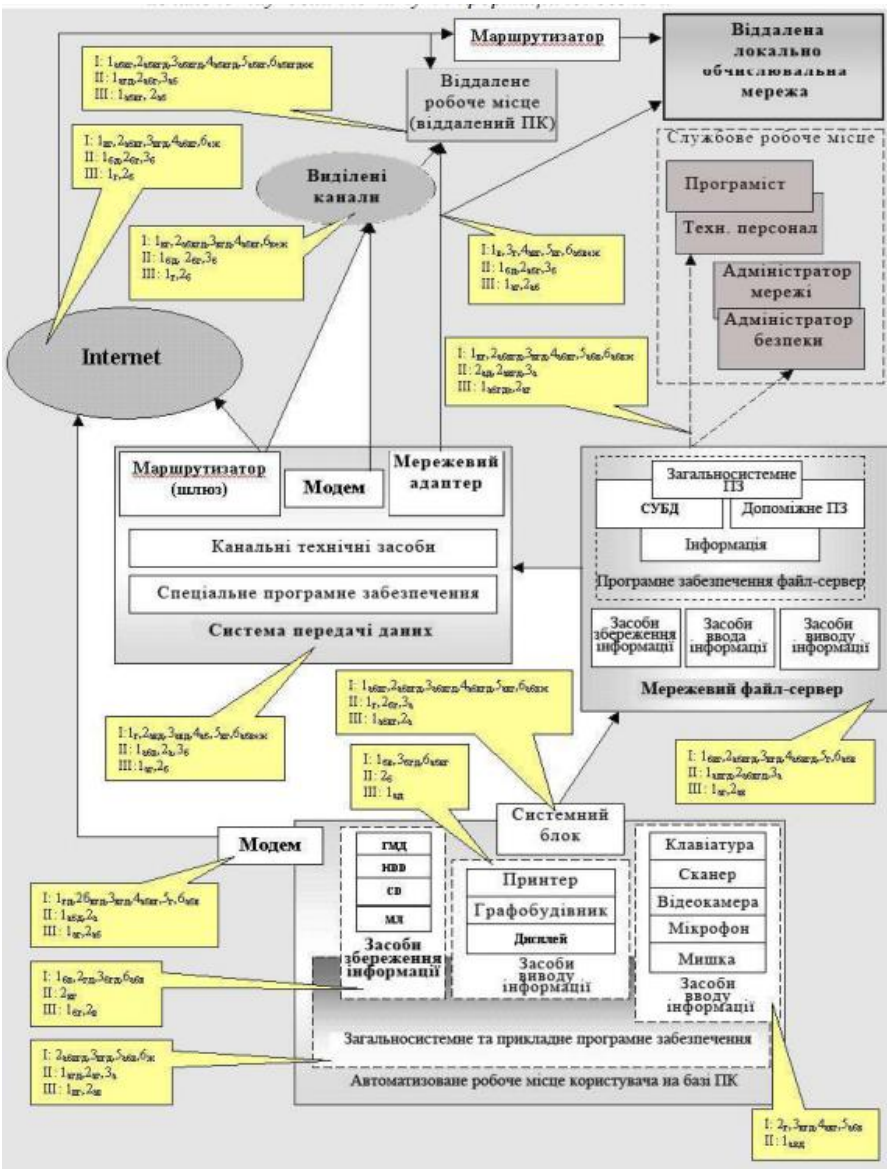
II. Загрози, що є наслідком відмов та збоїв технічних засобів - техногенні загрози;

III. Загрози, викликані стихійними джерелами - природні загрози.

Перша група найбільш велика й становить найбільший інтерес з погляду організації захисту цим загрозам, тому що дії суб'єкта завжди можна оцінити, спрогнозувати й вжити адекватних заходів.

Суб'єкти, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні, включаючи конкурентів, несумлінних партнери, політичних супротивників, так і внутрішні, що включають персонал установи та її філій (так звані, інсайдери).

З метою аналізу загроз комп’ютерній системі доцільно її відобразити у вигляді узагальненої схеми на якій може бути відображена сукупність потенційних загроз.



З метою аналізу загроз комп'ютерній системі доцільно її відобразити у вигляді узагальненої схеми на якій може бути відображена сукупність потенційних загроз.

Для кодифікації груп на згаданої схемі застосовані умовні позначення, що складаються з кількох елементів. Перший елемент – це римська цифра (I-III). Залежно від того, чи належить джерело загрози до антропогенної, техногенної або природньої категорії. Другій елемент – цифра (від 1-6) встановлює номер групи загроз залежно від класифікації наведеної нижче. Наступні елементи - букви кирилиці, що встановлюють зв'язок з відповідними підгрупами загроз

Наприклад, позначення на схемі - I.2абвг – означає загрози підгруп а),б),в) другої групи першої категорії до конкретно визначеного елемента комп'ютерній системи.

До першої категорії включимо загрози, що обумовлені діями суб'єктів, які можуть призвести до низки небажаних наслідків, серед яких стосовно корпоративної мережі, можна виділити наступні групи:

1. Крадіжка

а) технічних засобів (вінчестерів, ноутбуків, системних блоків);

б) носіїв інформації (паперових, магнітних, оптичних та ін.);
в) інформації (читання й несанкціоноване копіювання);
г) засобів доступу (ключі, паролі, ключова документація та ін.).
2. Підміна (модифікація):
а) операційних систем;
б) систем керування базами даних, прикладних програм;
в) інформації (даних);
г) заперечення факту відправлення повідомлень;
д) паролів і правил доступу.
3. Знищення (руйнування):
а) технічних засобів (вінчестерів, ноутбуків, системних блоків);
б) носіїв інформації (паперових, магнітних, оптичних та ін.);
в) програмного забезпечення (ОС, СУБД, прикладного ПЗ)
г) інформації (файлів, даних)
д) паролів і ключової інформації
4. Порушення нормальної роботи (переривання):
а) швидкості обробки інформації;
б) пропускної здатності каналів зв'язки;
в) обсягів вільної оперативної пам'яті;
г) обсягів вільного дискового простору;
д) електроживлення технічних засобів.
5. Помилки:
а) при інсталяції ПЗ, ОС, СУБД;
б) при написанні прикладного ПЗ;
в) при експлуатації ПЗ;
г) при експлуатації технічних засобів.
6. Перехоплення інформації:
а) за рахунок ПЕМВ від технічних засобів;
б) за рахунок наведень по лініях електроживлення;
в) за рахунок наведень по сторонніх провідниках;
г) по акустичному каналу від засобів виводу;
д) по акустичному каналу під час обговорення питань;
е) при підключенні до каналів передачі інформації;
ж) за рахунок порушення встановлених правил доступу (злом).

Друга категорія містить загрози, що прямо залежать від властивостей техніки. Технічні засоби, що містять потенційні загрози безпеці інформації так само можуть бути внутрішніми:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, застосовувані в установі;

і зовнішніми:

- засоби зв'язку;
- близько розташовані небезпечні виробництва;
- мережі інженерних комунікації (енерго- і водопостачання, каналізації);

- транспорт.

Наслідками застосування таких технічних засобів, що прямо впливають на безпеку інформації можуть бути:

1. Порушення нормальної роботи

а) порушення працездатності системи обробки інформації;

б) порушення працездатності зв'язку й телекомунікацій;

в) старіння носіїв інформації й засобів її обробки;

г) порушення встановлених правил доступу;

д) електромагнітний вплив на технічні засоби.

2. Знищення (руйнування)

а) програмного забезпечення, ОС, СУБД;

б) засобів обробки інформації (кидки напруг, протічки);

в) приміщень;

г) інформації (розмагнічування, радіація та ін.);

д) персоналу.

3. Модифікація (зміна)

а) програмного забезпечення. ОС, СУБД;

б) інформації при передачі по каналах зв'язку й телекомунікаціям.

Третю групу становлять загрози, які зовсім не піддаються прогнозуванню. Стихійні джерела, що становлять потенційні загрози інформаційної безпеки, як правило, є зовнішніми стосовно розглянутого об'єкта й під ними розуміються, насамперед природні катаклізми:

- пожежі;
- землетруси;
- повені;
- урагани;
- інші форс-мажорні обставини.

Ці природні й непередбачені явища так само впливають на інформаційну безпеку, небезпечні для всіх елементів корпоративної мережі й можуть призвести до наступних наслідків:

1. Знищення (руйнування)

а) технічних засобів обробки інформації;

б) носіїв інформації;

в) програмного забезпечення (ОС, СУБД, прикладного ПЗ);

г) інформації (файлів, даних);

д) приміщень;

е) персоналу.

2. Зникнення (пропажа)

а) інформації в засобах обробки;

б) інформації при передачі по телекомунікаційних каналах;

в) носіїв інформації;

г) персоналу.

У підсумку аналізу наведеної класифікації загроз безпеці інформації в комп’ютерній системі можливо зробити висновок, що її застосування під час формування вихідних даних для побудови системи захисту інформації дозволяє

впорядкувати роботу дослідника, уникнути зайвих витрат часу на збирання потрібних даних, зменшити ймовірність випадкових помилок та приділити особливу увагу вивченню та опису найбільш небезпечних загроз.

Загалом, наведена класифікація дозволяє, диференційовано підійти до розподілу матеріальних ресурсів, виділених на забезпечення інформаційної безпеки.

ТЕМА 4. Модель захисту та модель порушника в комп'ютерній системі

Класифікація автоматизованих систем в НД ТЗІ

В рамках нормативних документів системи технічного захисту інформації (НД ТЗІ) автоматизована система (АС) розглядається як організаційно-технічна система, що об'єднує програмне забезпечення (включаючи, операційну систему - ОС, прикладні програми), фізичне середовище, персонал і оброблювану інформацію.

Визначені складові можуть мати певні вразливості та бути об'єктами впливу зовнішніх та внутрішніх загроз, саме тому вимоги до функціонального складу комплексу засобів захисту в АС визначаються характеристиками оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги щодо рівня гарантій безпеки визначаються насамперед призначенням АС та важливістю оброблюваної інформації.

В НД ТЗІ залежно від сукупності характеристик АС (конфігурація програмного забезпечення, апаратних засобів і їх фізичне розміщення, види оброблюваної інформації, кількість користувачів і категорії користувачів) визначені три ієрархічні класи АС, вимоги до захисту яких істотно відрізняються.

До класу «1» віднесені комплекси у складі одного комп'ютеру (одно машинний) та одного користувача, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотною особливістю АС цього класу є вимога роботи з комплексом в кожний момент часу тільки одного користувача, хоча у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється. Також вимагається, що б всі технічні засоби АС, включаючи носії інформації, засоби її вводу/виводу, з точки зору захищеності належали одній категорії та використовуватись для оброблення всієї інформації.

Прикладом комплексу даного класу може бути комп'ютер, що не підключений до жодної мережі, крім живлення, та доступ до якого контролюється з використанням організаційних заходів.

До класу «2» віднесені локалізовані на певній контрольованій території комплекси, що обробляють інформацію різних категорій конфіденційності, за допомогою декількох фізично та логічно об'єднаних комп'ютерів до яких мають доступ для одночасної роботи декілька користувачів, що можуть здійснювати обробку інформації різних категорій конфіденційності.

Саме до цього класу можуть бути віднесені локальні обчислювальні мережі (ЛОМ).

Клас «3» це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотною відміною цього класу від класу «2» є необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Прикладом цього класу є глобальна мережа.

Практичному створенню систем захисту інформації в АС передує етап розробки ряду моделей для оцінки об'єктивних реальностей: загроз безпеки інформації, можливого порушника, моделі побудови й функціонування системи захисту. У відповідності з визначенням наукової філософії модель – деякий матеріальний або інший об'єкт, що є спрощеною версією об'єкта, що моделюється, або явища (прототипу) і в достатньому ступеню повторює властивості, істотні для цілей конкретного моделювання.

Застосування моделей, як спрощених описів важливих компонентів системи, дозволяє спростити розв'язок завдання створення адекватної реальним загрозам системи захисту, розбити цей процес на ряд етапів, провести попереднє дослідження, у тому числі із застосуванням комп'ютерної техніки, можливих варіантів побудови систем захисту, вивчити на моделі поведінки системи захисту в різних ситуаціях.

Розроблення моделі захисту та перенесення її на конкретну структуру програмних засобів, операційних систем, системи управління базами даних та на автоматизовану систему в цілому здійснюється на етапі проектування та техно-робочому етапі створення систем захисту.

Відповідні етапи передбачені державними стандартами на проведення дослідно-конструкторських робіт та нормативними документами системи технічного захисту, що встановлюють порядок створення комплексних систем захисту інформації.

Моделі захисту інформації

За суттю переважно більшість моделей захисту інформації базується на одному з двох базових методів розмежування доступу суб’єктів інформаційних систем до об’єктів дискреційному або мандатному.

Дискреційне або матричне (вибіркове) управління доступом (англ. Discretionary access control, DAC) — управління доступом суб’єктів до об’єктів на основі переліків управління доступом або матриці доступу.

Суб’єкт доступу «Користувач 1» має право доступу тільки до об’єкту доступу № 3, тому його запит до об’єкту доступу № 2 відхиляється. Суб’єкт «Користувач 2» має право доступу як до об’єкту доступу № 1, так і до об’єкту доступу № 2, тому його запити до даних об’єктів не відхиляються.

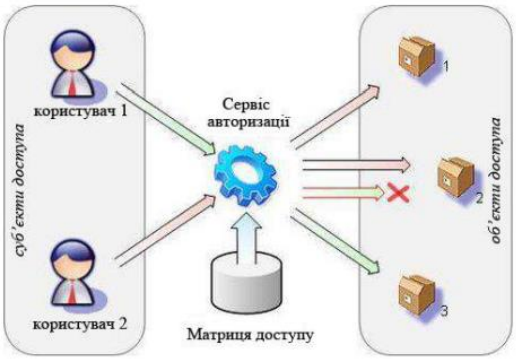


Схема дискреційної моделі управління доступом

Для кожної пари (суб’єкт – об’єкт) має бути заданий в явному вигляді перелік припустимих типів доступу (читати, писати тощо), тобто тих типів доступу, які є санкціонованими для даного суб’єкту (особи або групи осіб) до даного ресурсу (об’єкту).

Можливі декілька підходів до побудови дискреційного управління доступом:

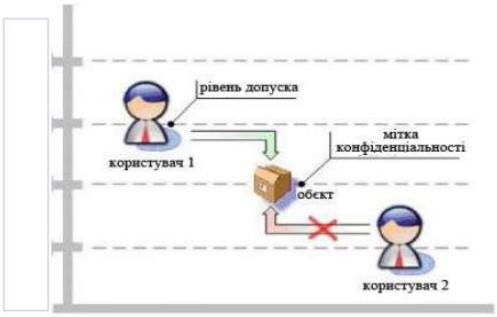
- кожен об’єкт системи має зв’язаного з ним суб’єкта, що називається власником. Саме власник встановлює права доступу до об’єкту;
- система має одного відокремленого суб’єкта - суперкористувача, який має право встановлювати права володіння для всіх інших суб’єктів;
- суб’єкт з визначеним правом доступу може передавати це право будьякому іншому суб’єкту.

Можливі також змішані варіанти побудови, коли одночасно у системі існують як власники, що встановлюють права доступу до своїх об’єктів, так і суперкористувач, що має можливість зміни прав для будь якого об’єкту та/або зміни його власника. Саме такій змішаний варіант реалізований у більшості операційних систем, наприклад, у класичних UNIX - системах або в системах Windows сімейства NT.

Дискреційне управління доступом є основною реалізацією політики розмежування доступу до ресурсів при обробці інформації з обмеженим доступом.

Мандатне управління доступом (англ. Mandatory access control, MAC) - це вид розмежування доступу суб’єктів до об’єктів, що заснований на призначенні позначки конфіденційності для інформації, що міститься в об’єктах, та видачі спеціального дозволу суб’єктам для поводження з інформацією такого рівня конфіденційності.

Цей метод, що поєднує захист і обмеження прав, застосовується по відношенню до обчислювальних процесів, даних та системних приладів автоматизованих систем та спрямовується на попередження порушень конфіденційності, доступності та цілісності інформаційних ресурсів.



Наведені на рисунку позначки мають наступне значення: ЦТ - цілком таємно, Т – таємно; ДСК – для службового користування; НС — не секретно.

У наведеному прикладі суб’єкт «Користувач 2», що має допуск рівня «не секретно», не може отримати доступ до об’єкту, для якого встановлена позначка «для службового користування». Водночас, суб’єкт "Користувач 1» с допуском рівня «таємно» має право доступу до об’єкту з позначкою «для службового користування».

Однієї з перших моделей захисту інформації в автоматизованій системі була опублікована в 1977 модель Біба (Віва). Згідно з нею всі суб'єкти й об'єкти попередньо розділяються по декільком рівням доступу, а потім на їхні взаємодії накладаються наступні обмеження:

- суб'єкт не може викликати на виконання об'єкти з більш низьким рівнем доступу;
- суб'єкт не може модифікувати об'єкти з більш високим рівнем доступу.

Модель Гогена-Мезигера (Goguen-Meseguer), що презентована в 1982 році, заснована на теорії автоматів. Згідно з нею система при кожній дії може переходити з одного дозволеного стану тільки в декілька інших. Суб'єкти й об'єкти в даній моделі захисту поділяються на групи – домени, при цьому перехід системи з одного стану в іншій виконується згідно з так званою таблицею дозволів, у якій визначено які операції може виконувати суб'єкт, скажемо, з домену А над об'єктом з домену В.

У даній моделі при переході системи з одного дозволеного стану в інше використовуються транзакції, що забезпечує загальну цілісність системи.

Сазерлендська (від англ. Sutherland) модель захисту, опублікована в 1986 році, побудована на взаємодії суб'єктів і потоків інформації. Так само як і в попередній моделі, тут використовується деякий автомат (машина) з кінцевою множиною дозволених комбінацій станів і деяким набором початкових позицій.

У цій моделі досліджується поведінка множинних композицій функцій переходу з одного стану в інші.

Важливу роль у теорії захисту інформації відіграє модель захисту КларкаВільсона (Clark-Wilson), опублікована в 1987 році й модифікована в 1989 році.

Заснована дана модель на повсюдному використанні транзакцій і ретельному оформленні прав доступу суб'єктів до об'єктів. Але в даній моделі вперше досліджена захищеність третьої сторони в даній проблемі – сторони, що підтримує всю систему безпеки. Цю роль в інформаційних системах звичайно відіграє програма - супервізор.

Крім того, у моделі Кларка-Вільсона транзакції вперше були засновані на методі верифікації, при цьому ідентифікація суб'єкта проводилася не тільки перед виконанням команди від нього, але й повторно після виконання. Це дозволило зняти проблему підміни автора в момент між його ідентифікацією й виконанням команди. Модель Кларка-Вільсона вважається однією із самих досконалих відносно підтримки цілісності інформаційних систем.

Модель порушника інформаційної безпеки

Запобігти потенційним та реальним загрозам у комп'ютерній системі, забезпечити надійний захист інформації можливо лише за умов визначення усіх потенційних та реальних категорій порушників, а також методів, які вони використовують.

Порушником будемо вважати особу, що випадково або усвідомлено з корисливих інтересів або без такого (наприклад, з метою самоствердження) здійснила спробу виконання заборонених у автоматизованій системі дій, використовуючи для цього різні методи та засоби.

Зловмисником, як і раніше, будемо називати порушника, що навмисно йде на порушення з корисливих спонукань.

Для визначення плану дій щодо захисту інформації в автоматизованій системі у кожній конкретній ситуації, виходячи з визначеної технологи обробки інформації, має бути визначена модель порушника, яка повинна адекватно відображати його можливості щодо втручання у роботу системи.

Неформальна модель порушника за суттю є описом його реальних або теоретичних можливостей, апріорних знань, технічної оснащеності, часу та місця дії тощо. Слід враховувати, що для досягнення своїх цілей порушник повинен прикласти деякі зусилля, затратити певні ресурси. Детально дослідивши умови порушень, у деяких випадках можна або вплинути на причини їх виникнення з метою їх усунення, або точніше визначити вимоги до системи захисту від даного виду порушень або злочинів.

Під час розробки моделі порушника встановлюються:

- припущення щодо категорії осіб, до яких він належить;
- припущення щодо мотивів та мети його дій;
- припущення щодо його кваліфікації та технічної оснащеності, застосованих методів та засобів;
- обмеження й припущення про характер можливих дій.

По відношенню до інформаційних ресурсів розрізнять категорії внутрішніх порушників (персонал підприємства) або зовнішніх порушників (сторонні особи). Внутрішнім порушником може бути особа з наступних категорій персоналу, що має доступ у будинки й приміщення, де розташовані компоненти автоматизованої системи:

- користувачі (оператори) автоматизованої системи;
- персонал, що обслуговує технічні засоби системи: інженери, техніки;
- співробітники відділів розробки й супроводження програмного забезпечення: системні та прикладні програмісти;
- технічний персонал, якій обслуговує будівлі: сантехніки, електрики, прибиральники тощо;
- співробітники служби охорони;
- керівники різних рівнів посадової ієрархії.

До сторонніх осіб, що можуть бути порушниками, слід віднести наступні категорії осіб:

- партнери підприємства або його клієнти - фізичні або юридичні особи;
- відвідувачі, що звернулися з власних справ або запрошені з будьякого питання;
- співробітники підприємств постачальників товарів та послуг, включаючи забезпечення життєдіяльності об’єкту інформаційної діяльності (зв'язок, ліфтове господарство, утримання систем сигналізації та відео спостереження, енерго -, водо -, теплопостачання тощо);
- співробітники підприємств – конкурентів, іноземні делегації;
- особи, випадково або навмисне порушили режим доступу на об’єкт інформаційної діяльності;

- співробітники дипломатичний місій або спецслужб. Останні можуть видавати себе за будь-яку категорію з тих, що перелічені вище;

- будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви порушень: недбалість (безвідповідальність), самоствердження (помста) і корисливий інтерес.

У випадку порушень, що обумовлені безвідповідальністю, користувач цілеспрямовано або випадково провадить які-небудь руйнуючі дії, не зв'язані проте зі злим наміром. У більшості випадків це слідство некомпетентності або недбалості.

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

Порушення безпеки інформаційної системи може бути викликане й корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для доступу до збереженої, переданої й оброблюваної у системі інформації.

Порушників можна класифікувати наступним чином.

За рівнем знань про інформаційну систему:

- знає функціональні особливості системи, 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 обслуговування;

- має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

- знає структуру, функції й механізм дії засобів захисту, їх сильні й слабкі сторони.

За рівнем можливостей та використовуваним методам і засобам:

- застосовує чисто агентурні методи здобування відомостей або втручання у роботу автоматизованої системи;

- застосовує нештатні пасивні методи та технічні засоби перехоплення інформації без модифікації компонентів системи;

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

- застосовує методи й засоби активного впливу на інформаційні ресурси, їх модифікації шляхом застосування спеціальних апаратно-програмних засобів, технічних приладів, які підключені до каналів передачі даних, впровадження програмних закладок, використання спеціального програмного забезпечення.

За часом дії:

- у процесі функціонування автоматизованої системи або її окремих компонентів;

- у період не активності компонентів системи, поза робочим часом, під час планових перерв у її роботі для обслуговування та ремонту тощо;

- як у процесі функціонування системи, так і в період не активності її компонентів.

За місцем дії:

- без доступу на контрольовану територію;
- з контрольованої території без доступу в будівлі та споруди;
- усередині приміщень, але без доступу до технічних засобів системи;
- з робочих місць кінцевих користувачів або операторів;
- з доступом у зону сховищ даних (ресурси, що знаходяться у статусі хостінгу, бази даних, архіви тощо);
- з доступом у зону керування засобами забезпечення безпеки.

В цілому, модель порушника, що побудована з урахуванням особливостей конкретної предметної області й технології обробки інформації, може бути представлена перерахуванням декількох варіантів його виду. Кожний вид порушника повинен бути охарактеризований значеннями характеристик, наведених вище.

Зокрема, нормативні документи системи криптографічного захисту інформації (КЗІ), залежно від вірогідних розумів експлуатації засобів криптографічного захисту інформації та відповідно до цінності інформації, що захищається, визначаються чотири рівні можливостей порушника:

нульовий рівень - ненавмисне порушення конфіденційності, цілісності та підтвердження авторства інформації;

перший рівень - порушник має обмежені засоби та самостійно створює засоби, розробляє методи атак на засоби КЗІ, а також інформаційно-телекомунікаційні системи із застосуванням широко розповсюджених програмних засобів та електронно-обчислювальної техніки;

другий рівень - порушник корпоративного типу має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

третій рівень - порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвиненої держави.

Слід звернути увагу, у силу непередбачуваності усіх можливостей порушника, навіть якщо у автоматизованій системі створюється комплекс засобів захисту, що роблять таке проникнення надзвичайно складним, повністю захистити її від проникнення «на всі 100%» практично неможливо.

Але система захисту повинна блокувати переважну більшість загроз безпеки інформації.

ТЕМА 5. Методи захисту інформації в комп'ютерних системах

Поняття та характеристика каналів витоку інформації

Під об'єктом інформаційної діяльності ми розуміємо впорядковану сукупність автоматизованих систем обробки інформації та засобів зв'язку деякого органу, підприємства або установи (далі – організація), допоміжних технічних засобів, персоналу організації, будівель та споруд зі інфраструктурою життєзабезпечення, території, на якій не може бути неконтрольоване перебування сторонніх по відношенню до організації осіб.

На об'єкті інформаційної діяльності може циркулювати як відкрита інформація, захист якої передбачений певними нормативними актами, так і інформація з обмеженим доступом.

Поточна діяльність організації звичайно потребує збору, зберігання, оброблення та обміну інформацією. Вказані дії можуть призводити до утворення певних умов для неконтрольованого розповсюдження інформації – її витоку за рахунок технічних каналів.

Залежно від природи походження розрізняють наступні типи каналів витоку інформації з обмеженим доступом:

- радіоканали;
- акустичні канали;
- електричні канали;
- візуально-оптичні канали;
- канали несанкціонованого доступу;
- матеріально-речові канали.

Привернемо увагу до особливостей перших двох, найбільш поширених на практиці та складних до блокування, каналів витоку інформації.

Виникнення радіоканалів витоку обумовлено випромінюванням різноманітними радіо та електроприладами електромагнітних хвиль у діапазонах від наддовгих з довжиною хвилі 10000 метрів (частоти менше 30 герц) до субміліметрових з довжиною хвилі 1—0,1 мм (частоти от 300 до 3000 гігагерц). Нагадаємо, що 1герц відповідає випадку одного коливання за секунду, 1 Гігагерц це вже 1мильйон коливань за секунду.

Залежно від властивостей, зокрема особливостей розповсюдження у просторі, під час розгляду електромагнітних випромінювань розрізняють декілька діапазонів хвиль: наддовгі, довгі, середні, короткі та ультракороткі хвилі.

Випромінювання з відносно великою довжиною хвилі (орієнтовно не менш 15-20 метрів) за рахунок відбиття від верхніх шарів атмосфери здатні розповсюджуватися на значні відстані, що перевищують сотні кілометрів. На відміну від них, випромінювання з довжиною хвилі, що не перевищує 10метрів, звичайно розповсюджуються в межах прямого зору на декілька десятків кілометрів.

На розповсюдження хвиль суттєво впливає наявність на їхньому шляху природних та штучних перешкод, суцільних конструкцій з бетону та металу. Можливість на певній відстані скористатися інформацією, які вони переносять,

також залежить від потужності випромінювання та рівня різного роду природних та штучних завад, які завжди присутні в ефірі. Зокрема, відповідні завади у містах утворюються обладнанням електротранспорту, електрозварювальними апаратами, роботою теле- та радіостанцій тощо.

Утворення побічних (не пов'язаних з безпосереднім функціонуванням обладнання) електромагнітних випромінювань у засобах електронної та електричної техніки обумовлюється низкою фізичних процесів у цих засобах. Наприклад, для отримання зображення на екрані монітору до нього подаються досить високі змінні напругі, що утворюють відповідні електромагнітні коливання, внаслідок чого може виникати радіоканал витоку інформації з обмеженим доступом.

Радіоканали витоку інформації отримали ще одну назву – канали побічних електромагнітних випромінювань та наведень (ПЕМВН).

Загально відомо, що слух людини є для нього другім по інформативності джерелом отримання відомостей про оточуючий світ. Під час проведення різного роду нарад, конференцій, тощо можуть обговорюватися відомості, що становлять таємницю, при цьому коливання молекул повітря, яке послідовно та синхронно зі звуком передається у просторі, призводить до виникнення акустичного каналу витоку інформації.

Якщо на шляху звуку не має перешкод, він рівномірно розповсюджується у всіх напрямках. У разі виникнення у певному напряму перешкоди у вигляді стін, вікон, стель, дверей, радіаторів опалення, інших конструкцій приміщень вони під тиском звукових хвиль також починають коливатися та передавати далі вказані інформативні сигнали.

Звичайна людина може почути звук у так званому звуковому діапазоні частот (від 16 до 20000 герц), діапазон звуків мови людини орієнтовно обіймає полосу частот лише від 100 до 6000 герц. Але ж у акустичному каналі перенесення інформації про роботу певних видів обладнання може відбуватися у більш широких межах: ультразвуковому (вище 20000 герц) та інфразвуковому (нижче 16 герц) діапазонах. У більш щільних та кристалічних середовищах (метал, камінь тощо) звук розповсюджується значно краще та на більшу відстань ніж в нещільних та аморфних середовищах.

Методи захисту інформації від НСД в автоматизованих системах

Раніше було відмічено, що для здійснення несанкціонованого доступу до інформації, оброблюваної в автоматизованих системах (НСД) зловмисник може не застосовувати спеціальні апаратні або програмні засоби, для цього він може використовувати:

- знання про інформаційну систему й уміння працювати з нею;
- відомості про слабості системи захисту інформації;
- збої, відмови технічних і програмних засобів;
- помилки, недбалість обслуговуючого персоналу й користувачів.

Для захисту інформації від НСД створюється система розмежування доступу до інформації. Одержати несанкціонований доступ до інформації при наявності системи розмежування доступу (СРД) можливо тільки при збоях і

відмовах системи, а також використовуючи вразливості в комплексній системі захисту інформації.

Для блокування несанкціонованого дослідження й копіювання інформації використовується комплекс засобів і заходів захисту, які поєднуються в систему захисту від дослідження й копіювання інформації (СЗК).

Таким чином, СРД і СЗК можуть розглядатися як підсистеми системи захисту від НСД.

Вихідною інформацією для створення СРД є рішення власника (адміністратора) системи про допуск користувачів до певних інформаційних ресурсів. Оскільки інформація в системі зберігається, обробляється й передається файлами (частинами файлів), тому порядок доступу до інформації регламентується на рівні файлів (об'єктів доступу).

Складніше організує доступ у базі даних, у яких він може регламентуватися до окремих її частин за певними правилами. При визначенні повноважень доступу адміністратор системи установлює операції, які дозволено виконувати користувачеві (суб'єктові доступу).

Розрізняють наступні операції з файлами:

- читання;
- запис;
- виконання програм.

Операція запису у файл має дві модифікації. Суб'єктові доступу може бути дане право здійснювати запис зі зміною вмісту файлу. Інша організація доступу припускає дозвіл тільки дописування у файл, без зміни старого вмісту.

В автоматизованих системах, залежно від особливостей їх реалізації застосовуються до організації розмежування доступу:

- матричний;
- повноважний (мандатний).

Матричне керування доступом припускає використання матриць доступу. Матриця доступу являє собою таблицю, у якій об'єкту доступу відповідає стовпець, а суб'єктові доступу рядок. На перетинанні стовпців і рядків записуються операції, які допускається виконувати суб'єктові доступу з об'єктом доступу.

Матричне керування доступом дозволяє з максимальною деталізацією встановити права суб'єкта доступу по виконанню дозволених операцій над об'єктами доступу. Такий підхід наочний і легко реалізується.

Однак у реальних системах через велику кількість суб'єктів і об'єктів доступу матриця доступу досягає таких розмірів, при яких складно підтримувати її в адекватному стані.

Повноважний або мандатний метод базується на багаторівневій моделі захисту. Документу присвоюється рівень конфіденційності (гриф таємності), а також можуть присвоюватися мітки, що відображають категорії конфіденційності (таємності) документа.

Таким чином, конфіденційний документ має гриф конфіденційності (конфіденційно, для службового користування, таємно, цілком таємно і т.д.) і може мати одну або кілька міток, які уточнюють категорії осіб, допущених до

цього документа (наприклад, «для керівного складу», «для інженернотехнічного складу» тощо).

Суб'єктам доступу встановлюється рівень допуску, що визначає максимальний для даного суб'єкта рівень конфіденційності документа, до якого дозволяється допуск. Суб'єктові доступу встановлюються також категорії, які пов'язані з мітками документа.

Правило розмежування доступу полягає в наступному: особа допускається до роботи з документом тільки в тому випадку, якщо рівень допуску суб'єкта доступу рівний або вище рівня конфіденційності документа, а в наборі категорій, привласнених даному суб'єктові доступу, утримуються всі категорії, певні для даного документа.

Система розмежування доступу до інформації може містити чотири функціональні блоки:

- блок ідентифікації й автентифікації суб'єктів доступу;
- диспетчер доступу;
- блок криптографічного перетворення інформації при її зберіганні й передачі;
- блок очищення пам'яті.

Ідентифікація й автентифікація суб'єктів здійснюється в момент їх доступу до пристроїв, у тому числі й дистанційного.

Диспетчер доступу реалізується у вигляді апаратно-програмних механізмів і забезпечує необхідну дисципліну розмежування доступу суб'єктів до об'єктів (у тому числі й до апаратних блоків, вузлів, пристроїв).

Якщо число спроб суб'єкта допуску одержати доступ до заборонених для нього об'єктам перевищить певну границю (звичайно 3-5 разів), то блок ухвалення рішення на підставі даних блоку реєстрації видає сигнал адміністраторові системи безпеки. Адміністратор може блокувати роботу суб'єкта, що порушує правила доступу в системі та з'ясувати причину порушень.

Крім навмисних спроб НСД диспетчер фіксує порушення правил розмежування, що з'явилися в наслідок відмов, збоїв апаратних і програмних засобів, а також викликаних помилками персоналу й користувачів.

Забезпечення доступності й цілісності інформації в АС

Підвищення надійності інформаційно-телекомунікаційних систем (ІТС), наприклад, дублювання джерел електроживлення та технічних засобів зберігання інформації на випадок їх відмови підвищує рівень безпеки інформаційних ресурсів, що обробляються цими системами. Під надійністю розуміється властивість системи виконувати покладені на неї завдання в певних умовах експлуатації.

У випадку відмови ІТС звичайно не здатна виконувати в повному обсязі передбачені технічною документацією функції, тобто переходить зі справного стану в несправний. Відновлення працездатності системи потребує певного часу, внаслідок чого що найменш призводить до не можливості скористатися її ресурсами. Ще гірше ситуація у випадку відмови накопичувачів інформації, оскільки в цьому випадку частина інформації втрачається назавжди.

Якщо при виникненні відмови деякого компонента система продовжує функціонувати, зберігаючи значення основних характеристик у визначених межах, то вважається, що вона перебуває в працездатному стані. Усунення відмови здійснюється без зупинки системи, втрат інформації не відбувається.

З погляду на забезпечення безпеки інформації необхідно зберігати хоча б працездатний стан системи. Для розв'язку цього завдання необхідно забезпечити високу надійність функціонування алгоритмів, програм і технічних (апаратних) засобів.

Оскільки алгоритми в ІТС реалізуються за рахунок виконання деяких програм на універсальних засобах обчислювальної техніки або спеціальними апаратними засобами, то надійність алгоритмів окремо не розглядається. У цьому випадку вважається, що надійність системи забезпечується надійністю програмних і апаратних засобів.

Звичайно, надійність системи досягається на наступних етапах її життєвого циклу (від створення до утилізації):

- розробки;
- виробництва;
- експлуатації.

Етап розробки програмних засобів є визначальним при створенні надійних інформаційних систем.

На цьому етапі основними напрямками підвищення надійності програмних засобів є:

- коректна постановка завдання на розробку;
- використання прогресивних технологій програмування;
- тестування та контроль правильності функціонування.

Різновидом надійних ІТС є відмовостійкі системи. Відмовостійкість – це властивість системи зберігати працездатність при відмовах окремих пристроїв, блоків, схем.

Відомі наступні основні підходи до створення відмовостійкіх систем:

- просте резервування;
- завадостійке кодування інформації;
- створення адаптивних систем.

Будь-яка відмовостйка система має надмірність. Одним з найбільш простих і діючих шляхів створення відмовостійких систем є просте резервування. Просте резервування засноване на використанні деякої кількості пристроїв, блоків, вузлів, схем тільки в якості резервних.

здійснюється на різних рівнях: на рівні пристроїв, на рівні блоків, вузлів і т.д. Резервування відрізняється також і глибиною.

Для цілей резервування можуть використовуватися один резервний елемент і більш. Рівні й глибина резервування визначають можливості системи нейтралізувати відмови, а також апаратні витрати. Такі системи повинні мати нескладні апаратно-програмні засоби контролю працездатності елементів і засоби переходу, при необхідності, на використання резервних елементів.

Прикладом резервування може служити використання «дзеркальних» накопичувачів на твердих магнітних дисках, систем резервного

електроживлення й т.п.. Недоліком простого резервування є непродуктивне використання засобів, які застосовуються тільки для підвищення відмовостійкості.

Помилки, обумовлені відмовами засобів системи, можна частково виправляти з використанням кодів, що виправляють помилки, - так званого завадостійкого кодування. Завадостійке кодування засноване на використанні інформаційної надмірності. При цьому кожен блок інформації в системі доповнюється певним обсягом спеціальної контрольної інформації. Наявність цієї контрольної інформації (контрольних двійкових розрядів) дозволяє шляхом виконання певних дій над робочою й контрольною інформацією визначати помилки й навіть виправляти їх.

Завадостійке кодування найбільш ефективне при ліквідації наслідків відмов, що самоусуваються, - так званих збоїв. Завадостійке кодування при створенні відмовостійких систем, як правило, використовується в комплексі з іншими способами підвищення відмовостійкості.

Найбільш досконалими системами, стійкими до відмов, є адаптивні системи. У них досягається розумний компроміс між рівнем надмірності, що вводиться для забезпечення стабільності (толерантності) системи до відмов, і ефективністю використання таких систем за призначенням.

В адаптивних системах реалізується так званий принцип елегантної деградації. Цей принцип припускає збереження працездатного стану системи при деякім зниженні ефективності функціонування у випадках відмов її елементів.

Одним з найефективніших способів забезпечення цілісності й доступності інформації в автоматизованих системах є її дублювання. Воно забезпечує захист інформації як від випадкових загроз, так і від навмисних впливів.

Залежно від цінності інформації, особливостей побудови й режимів функціонування інформаційних систем можуть використовуватися різні методи дублювання, які класифікуються по різних ознаках.

За часом відновлення інформації методи дублювання можуть бути розділені на:

- оперативні;
- неоперативні.

До оперативних методів належать методи дублювання інформації, які дозволяють використовувати дублюючу інформацію в реальному масштабі часу. Це означає, що перехід до використання дублюючої інформації здійснюється за час, який дозволяє виконати запит на використання інформації в режимі реального часу для даної системи. Усі методи, що не забезпечують виконання цієї умови, відносять до неоперативних методів дублювання.

По застосованим для цілей дублювання методам відповідні засоби можна розділити на ті, що використовують:

- додаткові зовнішні запам'ятовувальні пристрої (блоки);
- спеціально виділені області пам'яті на незйомних машинних носіях;
- з’ємні носії інформації.

По числу копій методи дублювання діляться на:

- однорівневі;
- багаторівневі.

Як правило, число рівнів не перевищує трьох.

По ступеню просторової віддаленості носіїв основної й дублюючої інформації методи дублювання можуть бути розділені на наступні методи:

- зосередженого дублювання;
- розосередженого дублювання.

Для визначеності доцільно вважати методами зосередженого дублювання такі методи, для яких носії з основною й дублюючою інформацією перебувають в одному приміщенні.

Усі інші методи належать до розосереджених.

Відповідно до процедури дублювання розрізняють методи:

- повного або дзеркального копіювання;
- часткового копіювання;
- комбінованого копіювання.

При повному копіюванні дублюються всі файли. При дзеркальному копіюванні будь-які зміни основної інформації супроводжуються такими ж змінами дублюючої інформації. При такім дублюванні основна інформація й дубль завжди ідентичні.

Часткове копіювання припускає створення дублів певних файлів, наприклад, файлів користувача. Одним з видів часткового копіювання, що одержав назву інкрементного копіювання, є метод створення дублів файлів, змінених із часу останнього копіювання.

Комбіноване копіювання допускає комбінації, наприклад, повного й часткового копіювання з різною періодичністю їх проведення.

Нарешті, по виду дублюючої інформації методи дублювання розділяються на:

- методи зі стиском інформації;
- методи без стиску інформації.

Захист інформації від витоку за рахунок електричних та електромагнітних каналів

Побудова ефективних системи захисту інформації й дієвого керування ними базується на знанні основних особливостей різних методів і засобів захисту інформації. Наступний матеріал розкриває зміст основних технічних методів захисту інформації.

Захист інформації від витоку за рахунок ПЕМВН - це комплекс заходів, що виключає або суттєво знижує вірогідність витоку інформації з обмеженим доступом за межи контрольованої зони.

Усі методи захисту від ПЕМВН можна розділити на пасивні й активні. Пасивні методи забезпечують зменшення рівня небезпечного (інформативного) сигналу або зниження його інформативності.

Активні методи захисту спрямовані на створення електромагнітних завад, що утрудняють приймання й виділення корисної інформації з перехоплених порушником сигналів.

Пасивні методи захисту від ПЕМВН можуть бути розбиті на три групи:

- екранування;
- зниження потужності випромінювань і наведень;
- зниження інформативності сигналів.

Екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Під екрануванням розуміється розміщення елементів автоматизованої системи, що створюють електричні, магнітні й електромагнітні поля, у просторово замкнених конструкціях. Способи екранування залежать від особливостей полів, що створюються елементами системи при протіканні в них електричного струму.

Залежно від типу створюваного електромагнітного поля розрізняють наступні види екранування:

- екранування електричного поля (електростатичне);
- екранування магнітного поля (магнітостатичне);
- екранування електромагнітного поля (електромагнітне).

Екранування дозволяє не тільки захистити обладнання автоматизованих систем від випромінювання власних небезпечних сигналів, а й зменшити ризик небажаного впливу зовнішніх електромагнітних та акустичних полів.

Електростатичне екранування полягає у замиканні силових ліній деякого електростатичного поля через електропровідний шар екрану та відведенні наведених електричних зарядів на землю (заземлення). Таке екранування ефективно діє для усунення так званих ємнісних паразитних зв’язків, що утворюються за рахунок природних або штучних електричних конденсаторів.

Ефективність такого екранування максимальна для постійного струму або коливань звукової частоти, але зі зростанням частоти швидко знижується.

Магнітостатичне екранування базується на замиканні силових ліній магнітного поля небезпечного сигналу у матеріалі екрана, що має малий магнітний опір для постійного струму або коливань низьких частот.

З підвищенням частоти сигналу застосовується виключно електромагнітне екранування, що основане на ослабленні високочастотного електромагнітного поля полем протилежного напряму, що утворене у матеріалі екрану так званими вихровими струмами.

Якщо відстань між колами, вузлами або провідниками, що екрануються, складає до 10% від чверті довжини хвилі сигналу, вважається, що зв’язок між вказаними елементами реалізується за рахунок електричного та магнітного полів, а не внаслідок перенесення енергії у просторі електромагнітними хвилями. Це досить важливо, тому що дозволяє окремо розглядати екранування електричних та магнітних полів, а якщо переважає одне з двох полів, то придушувати інше не потрібно.

Окремо слід зазначити, що заземлення та металізація корпусів апаратури, а також її складових забезпечує ослаблення паразитних зв’язків і наведень між окремими колами електричних схем, а також забезпечують ефективне відведення наведених сигналів на землю.

До групи, що забезпечує зниження потужності випромінювань і наведень, включають наступні методи:

- зміна електричних схем пристроїв;

- використання оптичних інтерфейсів – оптичних перетворювачів сигналів;

- зміна конструкції пристроїв;

- використання фільтрів;

- гальванічні розв'язки в системі електроживлення.

Зменшення потужності побічних випромінювань шляхом змін (удосконалення) електричних схем передбачає використання електро- і радіоелементів з меншим випромінюванням, уникнення регулярності повторень в інформаційних сигналах, зміна форми (крутизни фронтів) сигналів, запобігання виникненню паразитної генерації.

Ефективним напрямом подолання ПЕМВН є використання оптичних каналів зв'язку. Волоконно-оптичні кабелі успішно використовуються для передачі інформації на великі відстані, практично не маючі (у разі правильної прокладки) каналів витоку. Вони забезпечують високу швидкість передачі й не піддані впливу електромагнітних перешкод. Крім того, передачу інформації в межах одного приміщення, навіть великих розмірів, можна здійснювати за допомогою бездротових систем, що використовують випромінювання в інфрачервоному діапазоні.

Зміни конструкції пристроїв зводяться до змін взаємного розташування окремих вузлів, блоків, кабелів, скороченню довжини електричних з’єднань.

Використання фільтрів є одним з основних способів захисту від ПЕМВН. Фільтри є пристроями на основі різних електричних компонентів, які встановлюються або усередині пристроїв та систем для усунення поширення й можливого посилення наведених побічних електромагнітних сигналів, або на виході у напряму ліній зв'язку, сигналізації та електроживлення. Фільтри розраховуються таким чином, щоб вони забезпечували зниження сигналів у діапазоні побічних наведень до безпечного рівня й не вносили істотних викривлень корисного сигналу.

Повністю виключається просочування побічних наведених сигналів у зовнішній ланцюг електроживлення у разі використання джерел живлення, у яких реалізована гальванічна розв'язка між первинним та вторинним ланцюгами.

Зниження інформативності сигналів ПЕМВН, що утрудняє їхнє використання при перехопленні, реалізується шляхом застосування:

- спеціальних схемних рішень;

- кодування інформації.

У якості прикладів зниження інформативності сигналів можна привести такі, як заміна послідовного коду оброблення інформації паралельним, збільшення розрядності паралельних кодів, зміна черговості розгорнення рядків на моніторі тощо. Ці заходи утрудняють процес одержання інформації з перехопленого зловмисником сигналу.

Активні методи захисту від ПЕМВН передбачають застосування електромагнітних генераторів випадкових або псевдовипадкових шумів, які маскують небезпечний сигнал.

Використовується просторове й лінійне зашумлення.

Просторове зашумлення здійснюється за рахунок випромінювання за допомогою антен електромагнітних сигналів у простір. Застосовується локальне просторове зашумлення для захисту конкретного елемента системи й об'єктове просторове зашумлення для захисту від побічних електромагнітних випромінювань усього об'єкта.

При локальному просторовому зашумленні використовуються прицільні перешкоди. Антена перебуває поруч із елементом, що захищається. Об'єктове просторове зашумлення здійснюється, як правило, декількома генераторами зі своїми антенами, що дозволяє створювати перешкоди у всіх діапазонах побічних електромагнітних випромінювань усіх випромінюючих пристроїв об'єкта.

Просторове зашумлення повинне забезпечувати неможливість виділення побічних випромінювань на фоні створюваних перешкод у всіх діапазонах випромінювання й, разом з тим, рівень створюваних перешкод не повинен перевищувати санітарних норм і норм по електромагнітній сумісності радіоелектронної апаратури.

При використанні лінійного зашумлення генератори прицільних перешкод підключаються до струмопровідних ліній для створення в них електричних перешкод, які не дозволяють зловмисникам виділяти наведені сигнали.

Слід звернути увагу, що екранування засобів, які обробляють та зберігають критичну інформації, застосовується також для їх захисту від зовнішньої загрози - блокування зловмисного впливу на електронні блоки й магнітні запам'ятовувальні пристрої потужними зовнішніми електромагнітними імпульсами й високочастотними випромінюваннями, що приводять до несправності електронних блоків, що стирають інформацію з магнітних носіїв інформації.

Методи захисту від витоку інформації за рахунок акустичних та оптичних каналів

Методи протидії підслуховуванню інформації з обмеженим доступом можна розділити на два класи. Такими є:

- методи захисту мовної інформації при передачі її по каналах зв'язку.
- методи захисту від прослуховування акустичних сигналів у приміщеннях.

Для захисту від прослуховування мовної інформації, під час її передачі по каналах зв'язку, використовуються методи зашумлення кабелів, аналогове скремблювання або шифрування. Принципи останнього будуть розглянуті при обговоренні методів криптографічного захисту інформації.

Під скремблюванням розуміється така зміна характеристик мовного сигналу, що перетворений сигнал займає таку ж смугу частот, як і відкритий, але зміст переговорів для сторонньої особи нерозбірливий та учасники розмови залишаються невпізнаними.

Аналогові скремблери перетворюють вихідний мовний сигнал шляхом зміни його частотних і часових характеристик.

Застосовуються кілька способів частотного перетворення сигналу:

- частотна інверсія (обернення) спектра сигналу;

- частотна інверсія спектра сигналу зі зсувом несучої частоти;

- поділ смуги частот мовного сигналу на піддіапазони з наступною перестановкою й інверсією.

Дискретизація мовної інформації з наступним шифруванням забезпечує найвищий ступінь захисту. У процесі дискретизації мовна інформація представляється в цифровій формі. У такому виді вона перетвориться відповідно до обраних алгоритмів шифрування, які застосовуються для перетворення даних у телекомунікаційній системі.

Захист акустичної інформації у виділених приміщеннях є важливим напрямком протидії підслуховуванню.

Існує декілька методів захисту від прослуховування акустичних сигналів:

- звукоізоляція й звукопоглинання акустичного сигналу;

- зашумлення приміщень або твердого середовища для маскування акустичних сигналів;

- захист від несанкціонованого запису мовної інформації на диктофон;

- виявлення й вилучення закладних пристроїв.

Разом з тим, основними заходами при захисті від підслуховування й запису конфіденційних переговорів виступають організаційні та технічні заходи.

Організаційні заходи передбачають проведення архітектурнопланувальних і режимних заходів.

Архітектурно-планувальні заходи ґрунтуються на висуненні та реалізації певних вимог на етапі проектування приміщень, що захищаються, або в період їх реконструкції з метою виключення або ослаблення неконтрольованого поширення звукових полів.

Режимні заходи передбачають суворий контроль перебування в охоронній зоні співробітників і відвідувачів.

Організаційно-технічні заходи припускають проведення заходів двох видів – пасивних (забезпечення звукоізоляції і звукопоглинання) і активних (забезпечення звукопридушення), а також їх комбінації.

Проведення пасивних заходів спрямоване на зменшення величини акустичного сигналу в місцях передбачуваного розташування технічних засобів зловмисника до рівня, що гарантує неможливість перехоплення такого сигналу.

Активні заходи захисту, засновані на звукопридушенні, дозволяють збільшити шуми на частоті приймання інформативного сигналу до значення, що забезпечує гарантоване порушення акустичного каналу витоку інформації.

Технічні заходи містять у собі проведення заходів із залученням спеціальних засобів захисту конфіденційних переговорів.

До спеціальних засобів і систем протидії підслуховування й запису належать:

- засоби й системи для виявлення електромагнітних полів моторів, що забезпечують просування записуючого носія;

- програмно-апаратні комплекси для виявлення диктофонів із флешпам'яттю;

- пристрої придушення диктофонів (високочастотний генератор, генератор потужних груп ультразвукових сигналів);

- системи протидії мобільним телефонам, що використовуються як підслуховуючи пристрої.

Спеціальні дослідження технічних засобів

З точки зору розвідки усі канали витоку відрізняються інформативністю, ступенем надійності існування в умовах випадкових та спеціальних перешкод, дальністю доступу, ризиком компрометації (розкриття). Залежно від умов обстановки вказані канали можуть комбінуватися та доповнювати один одного.

Відповідно, для організації захисту інформації найбільш суттєвими характеристиками каналів витоку є складність їх виявлення та блокування, вартісні показники проведення відповідних робіт та впровадження засобів захисту, можливі наслідки у разі реалізації загроз через наявні вразливості у системі захисту.

Виявлення потенційно небезпечних каналів витоку здійснюється під час проведення перед проектного обстеження (до початку створення системи захисту) об’єкту інформаційної діяльності та проведення спеціальних досліджень.

Результати спеціальних досліджень засобів використовують для вироблення рекомендацій та формування переліку заходів щодо усунення можливих каналів витоку.

Для захисту акустичної інформації від несанкціонованого запису необхідно виявити роботу записуючого пристрою й вжити ефективних заходів протидії його використанню. Для цього використовуються різного роду локатори та пристрої блокування.

Змістовний модуль 2. Криптографічний захист інформації. Системи кіберзахисту

ТЕМА 6. Методи криптографічного захисту інформації

Предмет та об'єкти дослідження в криптографії

Криптографія, як складова науки криптології, є методологічною основою створення й забезпечення функціонування систем захисту інформації що передається та обробляється в глобальних і корпоративних інформаційно-телекомунікаційних системах.

Предметом криптографії є розроблення та дослідження математичних методів перетворення інформації з метою забезпечення її конфіденційності, цілісності, та підтвердження авторства. Остання властивість підтверджує факт створення інформації певною особою. Інша галузь криптології – криптоаналіз застосовується спеціальними службами для створення та дослідження методів відновлення (розкриття) захищеної методами криптографії інформації.

Під криптографічним захистом інформації розуміється застосування математичних перетворень вихідної інформації за допомогою секретних параметрів – так званих ключів, у результаті якого вона або стає недоступною для ознайомлення й використання особами, що не мають на це повноважень, або будь-яка спроба її модифікації може бути встановлена за допомогою спеціальних перетворень і публічних даних.

Загалом, залежно від цілі та характеру перетворень вихідної інформації розрізняють чотири типа математичних перетворень інформації:

стискання даних, що забезпечує віддалення з інформації певної надлишковості та зменшення її об'єму для зменшення навантаження на канали зв'язку або для компактного збереження на машинних носіях;

кодування інформації, яке орієнтоване на узгодження виду її подання з вимогами каналу зв'язку (наприклад двійкове кодування) або виявлення та виправлення в інформаційних потоках помилок, що обумовлені природними або індустріальними перешкодами;

стеганографічні перетворення, які використовуються для приховування факту передавання інформації або її збереження на деякому носії. Сутність стеганографічних перетворень розглядаються у наступному розділі;

шифрування, та побудовані за аналогічними принципами формування та перевірка електронного цифрового підпису (ЕЦП).

Саме проблеми шифрування, формування та перевірки ЕЦП в центрі уваги теоретичної та прикладної криптології.

Процес шифрування вихідної інформації полягає в реалізації певних алгебраїчних, логічних та інших математичних її перетворень, у результаті яких зашифровані повідомлення мають вигляд беззмістовних хаотичних наборів символів (літер, цифр, двійкових кодів тощо).

Зазвичай, для шифрування інформації використовуються певний алгоритм перетворення та деякий змінний секретний параметр - ключ.

Вихідними даними для алгоритму шифрування служить інформація, що підлягає захисту: почтові повідомлення, файли, бази даних тощо.

Ключ містить керуючу інформацію, яка визначає вибір певного перетворення з досить великої множини різних варіантів. При цьому кількість варіантів суттєво перевищує обчислювальні можливості навіть найсучасніших суперкомп'ютерів у разі їх застосування для пошуку вихідного вигляду інформації за методом послідовного перебору всіх ключів.

Розрізняють пряме перетворення відкритого повідомлення в шифрований текст – зашифрування, а також зворотне – розшифрування.

ЕЦП є деяким набором даних, що логічно пов'язані з даними, які захищаються. ЕЦП, як аналог звичайного підпису людини під будь-яким документом, дозволяє контролювати цілісність повідомлень та підтверджувати їх належність певній особі.

На відміну від методів криптографічного захисту інформації, методи стеганографії дозволяють приховувати не тільки зміст повідомлення, що зберігається або передається, але й сам факт зберігання або передачі конфіденційної інформації.

Зміст процесу кодування інформації полягає у заміні значень блоків (слів) вихідної інформації кодовими означеннями. При кодуванні й зворотному перетворенні застосовуються математичні формули або попередньо розраховані таблиці (словники).

При цьому перелічені елементи є відкритими та загальнодоступними. В випадку завадостійкого кодування, що використовується для підвищення вірогідності передавання інформації по каналах зв'язку, обсяг початкової інформації збільшується на кількість так званих перевірочних символів.

Слід звернути увагу, що термін також кодування використовується в криптографії для приховування змісту інформації. В остатньому випадку код для забезпечення конфіденційності інформації зберігається у таємниці. Цей вид захисту інформації частіше застосовується у збройних силах та дипломатичному листуванні.

Стискання даних реалізується за допомогою відкритих алгоритмів, воно може бути віднесене до методів захисту інформації з певними застереженнями. Основною метою стискання є скорочення обсягу повідомлень, що зберігаються на машинних носіях. У той же час стисла інформація не може бути прочитана або використана без зворотного перетворення.

Навіть якщо тримати в секреті алгоритми стиску, то вони можуть бути порівняно легко розкриті статистичними методами обробки. Тому до стислих файлів конфіденційної інформації додатково застосовують шифрування.

Криптосистеми й загрози їх безпеки

Криптографічна система (далі - криптосистема) – це сукупність засобів криптографічного захисту інформації, необхідних ключів, нормативної, експлуатаційної, а також іншої документації, у тому числі такої, що визначає заходи безпеки, використання яких забезпечує належний рівень захищеності інформації, яка обробляється, зберігається й передається.

Криптосистема працює за певною процедурою, її елементами є:

один або декілька криптографічних алгоритмів, що забезпечують шифрування, формування та перевірку ЕЦП, автентифікацію учасників інформаційного обміну;

система генерації та управління ключами до вказаних алгоритмів.

На вхід криптосистеми подається відкритий текст, а її виходом є зашифрований текст (шифротекст).

У загальному випадку криптографічне перетворення інформації можливо подати у наступному вигляді:

C=E(M,Ke)

де символи у рівнянні визначають наступні елементи криптосистеми:

C – зашифроване повідомлення (від англійського cipher- шифр);

E – алгоритм криптографічного перетворення (від encryption - шифрування);

M – вихідне повідомлення, що підлягає зашифруванню (від message - повідомлення);

Ke - ключ зашифрування (від key - ключ).

Згідно із процедурою, спочатку відкритий текст за допомогою криптоалгоритму з деяким ключем перетворюється в шифротекст. Потім шифротекст передається адресатові, де за допомогою алгоритму зворотного криптографічного перетворення й ключа розшифровується для одержання відкритого тексту:

M=D(C,Kd)

де символи у рівнянні визначають наступні елементи криптосистеми:

D – зворотнє криптографічного перетворення (від decryption - розшифрування);

Kd – таємний параметр розшифрування.

Для забезпечення безпеки криптографічного перетворення встановлюється особливий порядок поводження з ключами, зокрема, хоча б один з них обов’язково зберігається у таємниці (у деяких системах – обидва).

Слід зауважити, що нерідко функції перетворення E,D різняться лише порядком виконання проміжних перетворень. Відповідно перше називається прямим перетворенням, друге – зворотнім.

Ключі зашифрування Ke та розшифрування Kd можуть співпадати або ні.

Якщо ключі зашифрування и розшифрування збігаються, або один з іншого може бути досить просто обчислений криптосистема називається симетричною або одноключовою.

Криптосистема має назву асиметричної, якщо ключ зашифрування і ключ розшифрування не співпадають, а процедура обчислення одного ключа на основі іншого є практично нерозв'язним завданням. Один з ключів, залежно від цілі застосування визначається як відкритий та зберігається відповідним чином, інший – зберігається в секреті.

Процедура, за якою працює криптосистема, також включає технологію створення ключів і їх розповсюдження між абонентами мережі зв’язку.

Засоби, що реалізують наведені перетворення отримали назву засобів криптографічного захисту інформації (ЗКЗІ) або шифраторів.

До ЗКЗІ належать пристрої шифрування, формування та перевірки електронного цифрового підпису, системи розпізнавання або автентифікації суб'єктів та об'єктів автоматизованих систем, а також обладнання генерації ключів. Якщо ЗКЗІ реалізує функцію шифрування його ще називають шифратором.

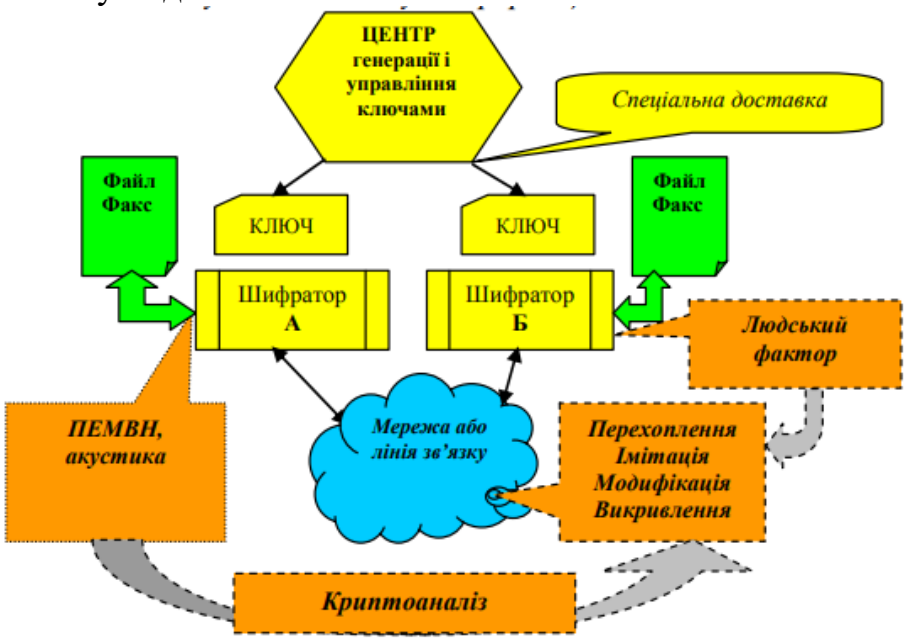
Залежно від способу реалізації та використаних технічних рішень розрізняють наступні типи засобів криптографічного захисту інформації:

- програмні, які реалізуються у вигляді програм, що виконуються на універсальних комп'ютерах (на відміну від спеціалізованих) під управлінням широко розповсюджених операційних систем Windows, Unix, iOS, Android тощо;

- програмно-апаратні, у яких переважна частина криптографічних перетворень реалізована у вигляді мікроелектронних пристроїв, що взаємодіють зі звичайними комп'ютерами за допомогою стандартних з'єднань, наприклад, інтерфейсу USB 2.0;

- апаратні, що побудовані у вигляді самостійних пристроїв, які відповідають певним схемно - технічним та конструктивним вимогам.

На рис. 1 наведена умовна структура криптосистеми, що включає два ЗКЗІ - шифратори абонентів мережі зв'язку А и Б, центр генерації та керування ключами і систему їх доставки.



Криптосистема за допомогою ключів забезпечує зашифрування вихідної інформації: даних, звуків, відео (англ. plaintext - відкритий текст) у нову послідовність (англ. ciphertext - шифрований текст), незрозумілу для третьої сторони; розшифрування відновлює початковий вигляд інформації.

Ключі не прописані "жорстко" у шифраторі, що дозволяє використовувати самі різні ключі, що згенеровані випадковим чином. Ключі розшифрування повинні зберігатися як секретні, щоб запобігти прослуховуванню каналу (eavesdropping) або розшифрування перехопленого зашифрованого тексту.

Загрозами для безпечного функціонування криптосистеми є можливості витоку критичної інформації від шифраторів по технічних каналах (ПЕМВН та акустика), перехоплення й маніпуляції інформацією в каналі, несумлінні дії персоналу.

Як було зазначено вище, нормативними документами системи КЗІ визначено чотири моделі порушника, тобто чотири рівня можливостей атакуючої сторони залежно від його технічної оснащеності, рівня знань та досвіду проведення крипто аналізу.

У загальному випадку криптографічна стійкість системи визначається її здатністю протистояти спробам атакуючої сторони, що перехопила шифрований текст і, що можливо має інформацію про відкрите повідомлення, відновити власне повідомлення або секретний ключ. Система ненадійна, якщо існують практично реалізовані методи визначення ключа й/або відкритого тексту на основі перехопленого зашифрованого повідомлення. Процеси (спроби) розкриття секретних параметрів криптосистеми й/або відкритого тексту називають криптоаналізом.

Під час оцінки рівня безпеки криптосистеми – її криптографічної стійкості вважається, що порушник системи безпеки має можливість перехоплювати усі шифровані повідомлення, що передаються, а також він знає принципи побудови застосованого криптографічного алгоритму.

Об’єктивно, криптостійкість системи залежить від числа її можливих ключів і використаного криптоалгоритму. Якщо довжина ключа в бітах є занадто короткою, то система може бути розкрита шляхом повного перебору (тобто послідовного випробування) усіх можливих ключів, поки не буде знайдений ключ, за допомогою якого перехоплене повідомлення розшифровується як якийсь відомий або значимий відкритий текст.

Наприклад, при довжині ключа 32 біта є приблизно 4 мільярди його варіантів. Сучасні суперкомп’ютери мають швидкодію, яка досягає декількох десятків трильйонів операцій в секунду. Вважаючи, що за секунду можна перевірити один мільйон ключів, отримаємо, що для перевірки 4 мільярдів ключів буде потрібно деяким більше години часу.

Навіть якщо довжина ключа досить довга, що атака повним перебором нездійсненна, криптосистема може бути вразлива до скороченого розв'язання, яке використовує слабості застосованої математики (алгоритму) системи або деяку лазівку в ній.

За одним виключенням, більшість криптосистем, принаймні, теоретично, уразлива щодо повного перебору ключів за наявності достатнього обчислювального ресурсу.

Теоретично не розкривається лише система з одноразовим використанням випадкової ключової послідовності, довжина якої дорівнює довжині вихідного повідомлення. Ця криптосистема отримала назву шифр Вернама по імені автора однієї з перших відомих реалізацій. Ключ у такій системі не може бути використаний двічі, у іншому випадку стійкість не гарантується.

Відомо, що у комп'ютерних системах кожен символ кодується 8 бітами. У цьому випадку в разі застосування шифру Вернама послідовність біт вихідного

повідомлення складається побітно із ключовою послідовністю за допомогою функції "виключне або" ("eXclusive OR" – XOR, або додавання за модулем 2) за правилом: 0⊕0 = 0, 0⊕1=1, 1⊕0 =1, 1⊕1= 0 , де: ⊕ позначає операцію XOR

Наприклад, у такий спосіб для відкритого тексту, що починається із символу N отримаємо:

Повідомлення - 01001000 …

Ключ - 11010001 …

Зашифрований текст - 10011001 …

Розшифрування здійснюється аналогічно, за винятком того, що ключ складається з бітами шифрованого тексту. Друге додавання із ключовою послідовністю відновлює вихідне повідомлення, тому що операція XOR "знищує" двічі застосований ключ k: ((m⊕k)⊕k)mod 2 = (m⊕2·k)mod 2 = m.

Стійкість системи з одноразовими ключами базується на неможливості одержання необхідної інформації про ключ або відкритий текст на основі перехопленого шифрованого тексту.

Система з одноразовими ключами та подібні, що використовують псевдовипадковий генератор ключової послідовності, належать до так званого класу потокових шифрів.

У потоковому шифрі одиницею (елементом) шифрування є один символ (літера, цифра, біт), на відміну від яких у блоковому шифрі елементом шифрування є послідовність від двох і більше символів. Відповідно розрізняють потокові та блокові криптоалгоритми.

Поряд з теоретичною стійкістю в криптології також розглядають практичну стійкість криптоалгоритмів. При цьому, криптосистеми, що теоретично вразливі та потенційно можуть бути дешифровані, вважаються практично стійкими, якщо ця стійкість базується на значної обчислювальній складності розв'язку певних математичних задач і занадто високої вартості засобів або ресурсів (включаючи часові), необхідних для їхнього розв'язку.

Практична стійкість криптосистеми має бути порівнянна з можливими ризиками для інформації й наслідками "злому". Витрати на криптосистему повинні враховувати сукупні збитки від "злому" системи.

Симетричні криптографічні системи

Розрізняють чотири типи криптографічних систем:

- симетричні (одно ключові) або із секретними ключами;
- асиметричні або с відкритими ключами;
- комбінація двох попередніх систем;
- системи генерації й керування ключами.

В одноключовій криптосистемі ключі зашифрування й розшифрування зберігаються як секретні, при цьому вони збігаються або нескладно обчислюється один з іншого.

Наприклад, нехай символи вихідного повідомлення (англ. message) M=m1,m2m3…. були замінені (зашифровані) за правилом ck=X(mk) для одержання шифротексту C=c1,c2,c3 … за допомогою двох рядкової таблиці – так званої підстановки X, яка наприклад, для латинського алфавіту може мати вигляд:

$$X = \begin{pmatrix} a\,b\,c\,d\,e\,f\,g\,h\,i\;j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z \\ d\,e\,f\,g\,h\,i\;j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z\,a\,b\,c \end{pmatrix}$$

При цьому відкритому символу m1=a відповідає символ зашифрованого тексту c1=X(a)=d.

Ключем даного симетричного криптоалгоритму, який ще називається шифром заміни або шифром Цезаря, є підстановка X. Ключ розшифрування (позначається X-1) утворюється простою зміною рядків у вихідній підстановці. Таким чином, ключ розшифрування (зворотна підстановка) має вигляд:

$$X^{-1} = \begin{pmatrix} d\,e\,f\,g\,h\,i\;j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z\,a\,b\,c \\ a\,b\,c\,d\,e\,f\,g\,h\,i\;j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z \end{pmatrix}$$

Оскільки до середини 70 років минулого століття усі відомі криптосистеми були одноключовими, то їх нерідко називають традиційними або звичайними.

У випадку одноключової системи, доставка ключів абонентам захищеного зв'язку здійснюється по деякому захищеному каналу або спеціальною службою доставки.

Необхідність створення та утримання відповідного каналу доставки секретних ключів є недоліком одноключової криптосистеми. Однак цей недолік компенсується більш високою криптографічною стійкістю порівняно із системами інших типів.

Як уже було відмічено вище, поряд з конфіденційністю, важливими вимогами до захищеного зв'язку є контроль цілісності, а також забезпечення справжності повідомлень - захист від фальсифікації або імітації.

За умов виконання певних вимог одноключові криптосистеми можуть забезпечити певний рівень стійкості щодо загрози підробки.

За умов виконання певних вимог одноключові криптосистеми можуть забезпечити певний рівень стійкості щодо загрози підробки. Стійкість у цьому випадку базується на тому, що для зміни шифрованого тексту, для якого при розшифруванні був би отриманий семантично значимий відкритий текст, необхідне знання секретного ключа.

У випадку неможливості автоматичного розпізнавання відкритого тексту або перевірки його значимості в системі може використовуватися код справжності повідомлення MAC (англ. message authentication code або імітовставка), який додається до повідомлення.

Обчислений за допомогою практично стійкого симетричного крипто алгоритму код MAC є функцією всього повідомлення й секретного ключа, що забезпечує практичну неможливість знайти інше повідомлення з тим же самим кодом (імітовставкою). Використовуючи той же самий секретний ключ, адресат (одержувач) обчислює MAC і перевіряє дійсність повідомлення шляхом порівняння обчисленого й отриманого MAC.

MAC може використовуватися для перевірки дійсності як відкритих (незашифрованих) повідомлень, так і для зашифрованих. Національними й міжнародними організаціями встановлені відповідні стандарти для MAC.

Одноключові системи нерідко використовуються для підтвердження належності користувачів до однієї системи (розпізнання), інакше - автентифікації.

Зокрема, в захищених системах паролі доступу, можуть зберігатися у зашифрованому вигляді. У цьому випадку шифрування використовується в якості односпрямованої (складно зворотної) функції для секретної інформації – паролю доступу. Недоліком цього методу є неможливість відновити пароль та необхідність його заміни за допомогою адміністратора системи.

Зважаючи на необхідність забезпечення сумісності захищених систем у різних сферах суспільного життя, зокрема, у банківському секторі, за ініціативою Національного інституту стандартів США в 1977 році корпорацією IBM був розроблений і прийнятий NIST в якості стандарту FIPS PUB 46-1 алгоритм шифрування DES (англ. Data Encryption Standart). DES є першим офіційним відкритим алгоритмом блокового шифрування інформації.

В алгоритмі DES початкове повідомлення подається у вигляді блоків довжиною 64 біт, які послідовно зашифровуються з використанням 56-бітного ключа. Кожен вихідний блок в алгоритмі після початкової перестановки біт проходить 16 ітерацій (раундів) перетворень за так званою схемою Фейстеля й потім піддається заключній перестановці, після чого утворюється блок зашифрованого тексту.

На кожній ітерації шифрується лише половино блоку, для чого до неї побітно за функцією XOR додається ключ раунду, результат перемішується за допомогою так званих S-боксів (блоків 4 бітових підстановок). Наприкінці раунду зашифрована та незашифрована половини блоку міняються місцями. Після чого виконується наступний раунд.

Стійкість алгоритму залежить від S-боксів, числа ітерацій, і довжини ключа (56 бітів дають приблизно 72,058 трильйонів варіантів ключів). Хоча алгоритм загальнодоступний, принципи побудови S-боксів тривалий час офіційно не опубліковувалися. Відомі реалізації алгоритму DES у вигляді чипа забезпечують шифрування з достатньо великою швидкістю - близько 200 Мб/сек.

DES може використовуватися у наступних режимах (це також має місце для інших алгоритми блокового шифрування):

1. Електронна кодова книга (ECB), при цьому забезпечується шифрування 64 бітних блоків шляхом їхньої заміни по підстановці.

2. Зворотний зв'язок по виходу (OFB), коли DES використовується в якості генератора псевдовипадкового ключової послідовності, яка складається по модулю 2 з потоком біт повідомлення (псевдомодель системи Вернама). Ключовий потік біт генерується DES за допомогою секретного ключа шляхом шифрування спочатку 64 бітного вектора ініціалізації, а потім зрушеного на один крок вектора з доповненням розряду, що звільнився, бітом ключа попереднього кроку шифрування.

3. Зворотний зв'язок по шифрованому тексту (CFB), збігається з попереднім режимом, за винятком того, що, звільнений після зрушення вектора ініціалізації розряд заповнюється бітом шифрованого тексту.

4. Зчеплення блоків шифрування (CBC), що представляє собою зміну блоків відкритого або шифрованого тексту шляхом їхнього підсумовування по модулю 2 з 64 бітними блоками, зашифрованими на попередньому кроці.

DES був прийнятий як урядовий стандарт, для захисту чутливої, але не класифікованої інформації (не віднесеної до категорії до державної таємниці) по прийнятій у США термінології.

Стандарт широко був поширений поза урядовою сферою, особливо в банківській системі. Американським національним інститутом стандартів (ANSI) прийнятий ряд стандартів, пов'язаних із шифруванням, включаючи керування доступом і розподіл ключів при використанні DES.

На заміну стандарту DES був прийнятий більш досконалий алгоритм AES, який є симетричним блоковим алгоритмом шифрування, що перетворює 128 біт вихідного блоку в блок шифрованого тексту довжиною 128 біт. Довжина ключа шифрування дорівнює 256 біт (можливі ключі довжиною 128 або 192 біта). Алгоритм може використовуватися в одному із чотирьох режимів, визначених в опису DES.

Алгоритм розроблений з використанням сучасних математичних методів для максимального прискорення його роботи на засобах обчислювальної техніки.

Державний стандарт - алгоритм ДСТУ ГОСТ 28147:2009 був розроблений в 1989 году, за принципом побудови (схема Фейстеля), розміру блоку, наявності блоку підстановок – аналога S-боксів досить схожий на алгоритм DES. Але на цьому перерахування загальних ознак можна, мабуть, закінчити. Тому що в іншому вони суттєво різняться.

Ключ довжиною 256 біт, можливість зміни блоку підстановок (потужність множини ключів має порядок 1089), 32 циклу перетворень проти 16 в американському варіанті забезпечують практично «непробивну» стійкість. Досить тільки вміло скористатися всім наявним потенціалом.

Швидкість шифрування за цим алгоритмом суттєво уступає DES, однак, завдяки певним схемно-технічним хитрощам – конвеєрному принципу побудови його вузлів – можна забезпечити досить високу продуктивність.

На основі аналізу даних з різних джерел для орієнтовної оцінки властивостей криптоалгоритмів визначені й пропонуються до розгляду чотири класи (рівня) стійкості (таблиця 1). Кандидати для включення у відповідні класи названі умовно, тому що для деяких з алгоритмів дотепер не доведена відсутність методів, що дозволяють суттєво спростити розв'язок задачі розкриття ключа.

Таблиця 1 Характеристика практичної стійкості симетричних алгоритмів

Рівень стійкості	**Кількість варіантів ключа**	**Довжина ключа**	**Криптоалгоритми що відповідають вимозі**
Низький	до 10^{24}	до 80 біт	*DES, FEAL, Skip Jack*
Середній	від 10^{25} до 10^{38}	від 80 до 128 біт	*Triple DES, IDEA, RC-6*
Високий	від 10^{39} до 10^{77} і більш	понад128 біт	*Blowfish, AES,* ГОСТ 28147-89
Абсолютний	одноразовий ключ	Довжина ключа дорівнює довжині повідомлення	шифр Вернама

Слід підкреслити, що границі класів необхідно переглядати з урахуванням розвитку обчислювальних можливостей комп'ютерної техніки.

Процедури й засоби генерації ключової інформації є одними з найбільш критичних елементів криптографічного захисту інформації.

Саме тому стандартом ДСТУ ГОСТ 28147:2009 і Інструкцією, що встановлює порядок постачання ключів до ЗКЗІ, які реалізують зазначений стандарт, передбачені додаткові особливі умови забезпечення безпеки інформації.

Згідно із цими умовами довготермінові ключові елементи для алгоритму ДСТУ ГОСТ 28147:2009 виготовляються й постачаються Держспецзв'язком України. Разові (сеансові) ключі можуть як поставлятися цим державним органом, так і генеруватися самим користувачем на основі методик погоджених із зазначеною структурою.

Підсумовуючи викладене можливо зробити висновок, що на поточний момент теорія і практика застосування симетричних криптографічних систем достатньо глибоко опрацьовані, що дозволяє будувати ефективні надійні криптосистеми.

ТЕМА 7. Криптографічні системи з відкритим розподілом ключів

Застосування криптосистем з відкритими ключами

У криптосистемі, що заснована на відкритому розподілі ключів (асиметричній системі) кожний користувач або застосування мають пару постійно або довгостроково використовуваних ключів: відкритий і секретний (ще особистий) ключі.

Відкритий ключ може бути вільно розповсюджений, припустиме його зберігання в загальному каталозі, але секретний ключ повинен бути доступний тільки користувачеві або шифратору користувача. Оскільки відкритий і секретні ключі математично зв'язані, то функція повинна бути такою, що за прийнятний час секретний ключ не може бути обчислений виходячи з відкритого ключа.

Система з відкритими ключами дозволяє кожній зі сторін інформаційного обміну установити спільне значення секретного сеансового ключу без попереднього його розсилання секретною поштою.

При цьому кожний шифратор генерує випадковим образом секретний (особистий) ключ. Потім, за допомогою так званої односпрямованої функції обчислюється відкритий (публічний) ключ. Односпрямована функція в обчислювальнім відношенні важко оборотна, так що секретний ключ практично не може бути обчислений на основі відкритого ключа.

Далі шифратори обмінюються відкритими ключами. На основі отриманого відкритого ключа й власного секретного кожний із шифраторів обчислює спільний сеансовий ключ. Таким чином, ключ сеансу є функцією обох секретних ключів. сторона, що підслуховує, не може відновити сеансовий ключ.

Перевага криптосистем з відкритим ключем - це можливість обміну по незахищеному каналу інформацією, необхідної для роботи шифраторів. Недолік – використання гіпотетичного об'єкта: односпрямованої функції, для якого не доведена відсутність алгоритмів розв'язку задачі знаходження зворотного значення за приємний час.

До початку використання ГОСТ 28147-89 або DES, як втім і будь-якої іншої симетричної криптографічної системи, щоб зашифрувати повідомлення, обидві сторони інформаційного обміну: адресант (відправник) і адресат (одержувач) повинні домовитися про секретні ключі сеансу - ключі шифрування в кожному напрямку. Процес визначення сеансового ключу називається ключовим обміном або розподілом ключів.

Перша схема відкритого розподілу ключів була запропонована У.Диффі й М.Хеллманом. Рис.8.1 пояснює принципи формування загального ключа за схемою Диффі-Хеллмана.

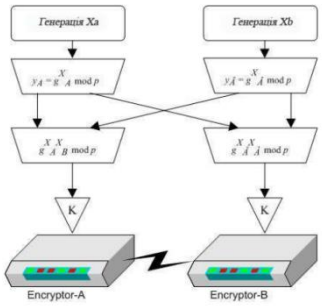


Рис. 8.1. Формування спільного ключу за схемою Диффі-Хеллмана

У цьому прикладі, абонент А генерує випадковий секретний ключ xA, а абонент В генерує випадковий секретний ключ xb. Потім кожна зі сторін обчислює відкритий ключ, відповідно ya по xA й yb по xb, які направляються по каналу зв'язку іншій стороні, на основі яких обчислюється загальний ключ сеансу.

У такий же спосіб, криптосистема, заснована на використанні відкритих ключів, може бути використана для формування сеансових ключів для симетричної криптосистеми в обох напрямках передачі.

Схема зв'язку в цьому варіанті виглядає в такий спосіб: для відправлення повідомлення, адресант одержує відкритий ключ адресата й використовує його, для зашифрування повідомлення. Адресат розшифровує повідомлення, використовуючи свій секретний ключ. Ключі адресата використовуються для відповіді.

Хоча в теорії x можна знайти за зв'язаним значенням y шляхом обчислення дискретного логарифма (тобто, log y mod p), але практично для великого p (від 700 і більш біт) це вимагає величезних обчислювальних ресурсів.

Криптосистема RSA. RSA - криптосистема з використанням відкритих ключів, названа по перших буквах імен її творців.

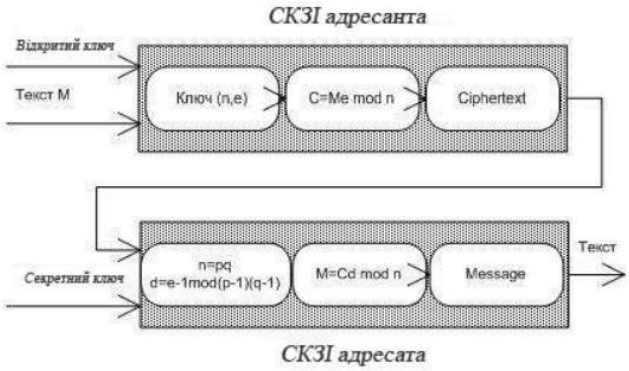


Рис. 8.2 Схема шифрування за алгоритмом RSA

Зашифрування й розшифрування в RSA реалізуються піднесенням у ступінь блоку повідомлення великої довжини в кінцевій множині. Відкритими ключами системи є один з показників експоненти й модуль, що представляє собою добуток двох великих простих чисел. Відповідний секретний ключ включає інший показник експоненти й прості співмножники відкритого модуля. Послідовне застосування показників експонент відновлює первісне повідомлення (рис. 8.2).

Кожний абонент системи має пари - відкритий і секретний ключ, значення яких лежить у діапазоні від 1024 до 4096 біт модуля n, де n= pq із секретними p і q. Відкриті ключі: n і показник експоненти e; секретний ключ: прості числа p і q, а також секретний показник експоненти d, який є інверсією e за модулем mod (p -1) (q -1).

Секретні значення p і q потрібні тільки на етапі генерації інших параметрів - показників експонент - після їхнього створення p і q вони не використовуються. Для шифрування використовується відкритий ключ адресата. Відправник шифрує блок повідомлення M, зводячи його в ступінь e (mod n). Отримувач розшифровує блок, зводячи його в ступінь d (mod n). Розшифрування відновлює первісне повідомлення, у силу залежності між e і d має властивість: (Me mod n)d (mod n) = (Med mod n) = M.

Відзначимо, що авторами системи був запропонований розмір ключа від 512 до 1024 біт. Однак можна помітити, що складність задачі базується саме на розкладанні більших чисел на множники. З моменту появи системи одинаками й цілими колективами постійно проводилися атаки шляхом повного або оптимізованого перебору.

За рахунок використання зроблених методів факторизації й високопродуктивних комп'ютерів задача розкладання вже впевнено зважується на рубежі 700 бітних чисел, Для великої кількості комп'ютерів (порядку 1000) і застосування методів розпаралелювання обчислень забезпечена факторизація чисел розміром 900 біт.

Для виключення можливості реалізації загроз, вочевидь, настав час застосовувати числа що найменш 1024 біт або більше, розкладання на множники яких найближчим часом представляється проблематичним.

Реалізація криптосистеми RSA вимагає значно більшу кількість обчислювальних ресурсів, чім симетричні системи, що використовують, зазвичай, прості перестановки й заміни біт. Із цієї причини, RSA не використовується безпосередньо для зашифрування даних великої довжини.

Система знайшла практичне застосування в комбінації із симетричними криптосистемами для розподілу ключів для останніх по незахищених каналах. Для відправлення зашифрованого повідомлення адресант генерує сеансовий ключ для симетричної системи, за допомогою якого шифрує своє повідомлення, потім шифрує сеансовий ключ за допомогою відкритого ключа системи RSA.

Зашифрований секретний ключ і повідомлення відправляються адресатові. На прийомному кінці процедура виконується у зворотному порядку: розшифрування секретного ключа, зашифрування з його допомогою власне повідомлення.

Ця процедура реалізується у багатьох протоколах захищеного інформаційного обміну. Зокрема, відомий стандарт Интернет PEM (Internet Privacy Enhanced Mail) для захисту електронної пошти крім симетричного алгоритму шифрування згідно стандарту DES використовує розподіл ключів за алгоритмом RSA.

Електронний цифровий підпис (ЕЦП) - це блок даних, логічно пов'язаний з однієї сторони з повідомленням (документом або файлом), з іншого боку - з

певною особою (або об'єктом), при цьому підпис може бути перевірений адресатом або незалежною третьою особою і практично не може бути підроблена. Цей зв'язок забезпечується засобом ЕЦП, що побудований на основі криптосистеми з відкритими ключами, та використовує пару - відкритий і особистий (секретний) ключ.

Для формування цифрового підпису повідомлення, адресант, використовуючи певну функцію (має назву хеш-функція), обчислює стислий образ повідомлення. Власне цифровий підпис формується на основі хеш-образу повідомлення за допомогою деякого криптографічного алгоритму та особистого ключа адресанта. Після об'єднання з повідомленням вона відправляється адресатові.

Для перевірки цілісності й справжності інформації отримувач формує хеш-образ отриманого повідомлення, який порівнює з результатом обертання ЕЦП за допомогою відкритого ключа відправника. Повідомлення може передаватися як у відкритому, так і зашифрованому виді, останній режим є більш кращим з погляду безпеки системи.

Цифровий підпис виключає невизнання особою, що підписує, відправленого повідомлення. Як наслідок, цифровий підпис може використовуватися при укладанні електронних контрактів, замовленні товарів в електронних магазинах і т.п. Крім того, цифровий підпис може підтверджувати цілісність і справжність програмного забезпечення й даних, ідентифікувати зображення, користувачів і апаратні засоби. Наприклад, смарт-карта, що реалізує функцію цифрового підпису, може використовуватися для автентифікації користувачів комп'ютерної системи.

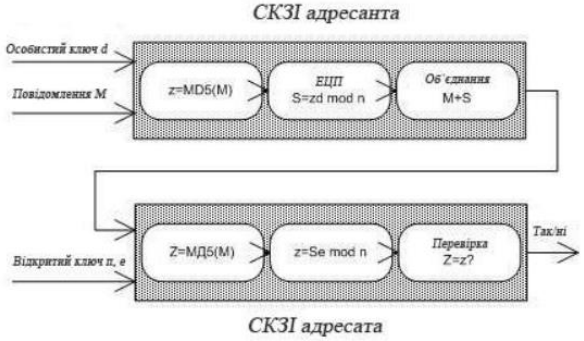


Рис. 8.3 Схема формування ЕЦП за допомогою алгоритму RSA

Алгоритм RSA також може застосовуватися для формування цифрового підпису. При цьому ключі використовуються трохи інакше, чим у випадку шифрування.

Рис. 8.3 пояснює, принципи формування ЕЦП за допомогою алгоритму RSA. Для підпису повідомлення і його перевірки використовуються параметри адресанта: модуль n і ступені експонент e і d. Щоб підписати повідомлення, відправник створює його хеш-образ z з використанням деякої хеш-функції (у наведеному прикладі - MD5).

Підпис формується шляхом піднесення образа в ступінь особистого ключа адресанта d (mod n). Отриманий підпис разом з повідомленням відправляється адресатові. На прийомному кінці розшифроване при необхідності повідомлення хешується, потім отримувач перевіряє правильність

підпису, зводячи його в ступінь відкритої експоненти e(mod n) і порівнюючи отриманий результат з обчисленим хеш-образом повідомлення.

В 1991 році NIST запропонував стандарт цифровому підпису (DSS) для урядових систем. DSS використовує алгоритм SHA-1 для хешування повідомлень перед підписом.

В 1995 році в РФ був розроблений стандарт цифрового підпису ГОСТ Р34.10 (в Україні має індекс 34.310) що реалізує так звану схему К.Шнорра побудовану на протоколі Ель-Гамаля.

DSS, і ГОСТ Р34.10 реалізують піднесення в ступінь більших чисел у модульній арифметиці. Розмір ключа - 512 або 1024 біта, стійкість визначається складністю розв'язку задачі дискретного логарифмування, що приблизно відповідає складності розв'язку задачі факторизації (розкладання на множники), тому стійкість DSS порівняння з RSA.

Усі асиметричні криптосистеми є об'єктом атак шляхом оптимізованого перебору ключів, що приводить до необхідності використання набагато більш довгих ключів, чому ті, які використовуються в симетричних криптосистемах, для забезпечення еквівалентного рівня захисту.

Це відразу ж позначається на обчислювальних ресурсах, необхідних для шифрування. Останнім часом активно розвивається напрямок, що пов'язаний з побудовою криптографічних алгоритмів, що використовують апарат еліптичних кривих (ECC). Саме застосування еліптичних кривих може пом'якшити проблему складності обчислень із багато розрядними числами.

Зокрема, в Україні прийнятий встановленим порядком державний стандарт ДСТУ 4145-2002, якій визначає алгоритм формування та перевірки ЕЦП на базі математичних перетворень із застосуванням еліптичних кривих.

У ряді видань наводяться дані про еквівалентні довжини ключів. З метою наочної демонстрації викладеного такі дані (умовно еквівалентні довжини ключів) наведено в таблиці 2.

Таблиця 2 – Еквівалентні довжини ключів

Довжина ключа симетричної системи (біт)	Кількість варіантів ключів	Довжина ключа RSA систем (біт)	Довжина ключа ECC систем (біт)
56-64	10^{17} -10^{19}	384-512	112
80	10^{24}	768	132
112	10^{34}	1792	160
128	10^{38}	2304	240

Хеш-функції є одним з важливих елементів криптосистем на основі ключів. Їх відносно легко обчислити, але майже неможливо розшифрувати. Вихідні дані хеш-функції мають змінну довжину, результат - рядок фіксованого розміру (часто називану дайджестом повідомлення - MD), звичайно довжиною 128…256 біт.

Найважливіша властивість хеш-функцій, використовуваних у системі цифрового підпису, це практична неможливість добору другого повідомлення, що має той же самий хеш-образ. Ця характеристика виключає можливість підміни повідомлення несправжнім з більш пізньою датою відправлення.

Крім того, повинне бути практично неможливо знайти два різні повідомлення, що хешуються у спільний образ. Це охороняє проти погрози генерації двох повідомлень, одне з яких підписується, а інше пред'являється як підписане.

У таблиці 3 наведені загальні характеристики відомих функцій хешування. Слід зауважити, що алгоритми хешування ГОСТ 34.311 і SHA-1, що стискають повідомлення до рядка біт фіксованої довжини, задовольняють обом вище наведеним умовам.

Таблиця 3 Характеристика хеш-функцій

Назва	**Характеристика функції**
ГОСТ 34.311	Державний стандарт України. Довжина дайджесту 256 біт . Використовується при створенні ЕЦП за стандартом ДСТУ 4145-2002. Для обробки блоків використовуються блоковий алгоритм шифрування ДСТУ ГОСТ 28147:2009.
SHA-1 (*Secure Hash Algorithm*)	Стандарт США, призначена для використання в стандарті цифрового підпису *DSS*. Створює 160-бітне значення дайджесту з вихідних даних змінного розміру.
RIPEMD-160	Міжнародний стандарт. Довжина дайджесту 160-біт. Має швидкодію на рівні алгоритму *SHA-1*. Використання не обмежене патентами.
*MD*5	Міжнародний стандарт. Довжина дайджесту 128 біт. Найпоширеніша з хеш-функцій. За рівнем безпеки поступається алгоритму *SHA-1* . На третину швидше чим *RIPEMD-160*. Забезпечує цілісність даних.

Управління відкритими ключами

Криптосистеми з відкритими ключами, у тому числі, що реалізують ЕЦП, процедури автентифікації, привабливі для користувачів у силу можливості забезпечення досить високого рівня безпеки за умови обміну тільки несекретною інформацією.

Однак, у цьому випадку, серйозним ризиком для безпеки системи, є можливість підміни відкритих ключів. Як варіант, зловмисник може зайняти місце легального користувача або підмінити його відкритий ключ своїм власним. У цьому випадку він може ввести в оману інших користувачів системи.

Для захисту від цієї загрози, відкриті ключі можуть розміщатися в підписаних електронних файлах - сертифікатах, використовуваних для перевірки дійсності ключів. Сертифікат за суттю є інформаційним полем, що містить необхідні дані для ідентифікації користувача системи інформаційного обміну, зокрема, що реалізує ЕЦП.

Перед використанням відкритого ключа перевіряється справжність його сертифікату, у т.ч. шляхом перевірки його підпису. Сертифікат звичайно містить ідентифікатор користувача, відкритий ключ і позначку часу його формування і терміну придатності.

Сертифікат підписується центром сертифікації ключів, чиї власні ключі можуть бути завірені повноваженнями органа сертифікації вищого рівня. Сертифікати передаються від центру сертифікації електронним шляхом.

При цьому ключі для зашифрування (відкритий) й розшифрування (секретний) різні, хоча й створюються разом. Один ключ стає відомим зацікавленим учасникам системи зв'язку, а інший зберігається в таємниці. Хоча можна шифрувати й розшифровувати обома ключами, дані, зашифровані одним ключем, можуть бути розшифровані тільки іншим ключем.

Для того щоб уникнути низької швидкості алгоритмів асиметричного шифрування, для кожного повідомлення генерується сеансовий (тимчасовий) ключ алгоритму симетричного криптоалгоритму.

Власне повідомлення шифрується з використанням цього тимчасового сеансового ключа й симетричного криптоалгоритму.

Потім цей сеансовий ключ шифрується за допомогою відкритого ключа отримувача й асиметричного алгоритму шифрування. Після чого зашифрований сеансовий ключ разом із зашифрованим повідомленням передається адресатові.

Адресат, використовуючи той же самий асиметричний алгоритм шифрування й свій секретний ключ, розшифровує сеансовий ключ, а з його допомогою розшифровується власне повідомлення.

В комбінованих криптосистемах важливо, щоб ключі симетричних і асиметричних алгоритмів були порівнянні відносно рівня безпеки, який вони забезпечують. Якщо використовується короткий сеансовий ключ (наприклад, 40-бітовий ключ для алгоритму DES), то практично не має значення, наскільки великі асиметричні ключі. Атаці будуть піддані не вони, а сеансові ключі DES.

Потрібно мати на увазі, що в комбінованій системі якщо атакуючій стороні стане відомий секретний ключ асиметричного шифрування, то буде скомпрометовано не тільки поточне, але й усі наступні повідомлення, відправлені адресатові.

Для організації захищеного інформаційного обміну в системі з відкритим розподілом ключів має бути створена певна система управління ключами, що отримала назву Інфраструктура відкритих ключів.

Сутність Інфраструктури відкритих ключів полягає в наступному.

1. Безпечно створюються й поширюються відкриті й секретні ключі асиметричних алгоритмів. Секретний ключ передається його власникові. Відкритий ключ зберігається в базі даних у стандарті X.500 і адмініструється центром сертифікації ключів (ЦСК, Certification Authority).

Вважається, що користувачі довіряють адміністрації системи в плані забезпечення безпеки створення, розподілу й адміністрування ключами, включаючи своєчасне знищення використаних ключів.

2. Для кожного повідомлення обчислюється його хеш-функція. Отримане значення з допомогу асиметричного алгоритму (наприклад, ДСТУ 4145-2002, RSA) і секретного ключа відправника (адресанта) перетворюється в ЕЦП повідомлення, а потім отриманий рядок символів додається до переданого тексту. Таким чином, тільки відправник може створити ЕЦП.

3. Далі, генерується секретний ключ симетричного криптоалгоритма, який буде використовуватися для шифрування тільки цього повідомлення або сеансу взаємодії (сеансовий ключ). Після чого повідомлення шифрується разом з доданим до нього електронним підписом за допомогою симетричного криптоалгоритма й разового (сеансового) ключа, внаслідок чого створюється шифротекст.

4. Тепер потрібно розв'язати проблему з передачею сеансового ключа одержувачеві повідомлення. Перехоплення незашифрованих запитів на одержання цього відкритого ключа є розповсюдженою формою атаки.

Відправник повинен одержати від ЦСК відкритий ключ адресата для асиметричного криптоалгоритму.

Для забезпечення безпеки та підтвердження дійсності відкритого ключа в ЦСК використовується система сертифікатів на основі стандарту X.509 описує формат їх подання та методи одержання користувачами від ЦСК відкритих ключів. Слід зазначити, що ця технологія не може з 100% гарантією захистити від підміни відкритого ключа, що є певним обмеженням для застосування систем з відкритим розподілом.

Отже, адресат запитує в ЦСК відкритий ключ одержувача повідомлення. Цей процес уразливий до атаки, у ході якої атакуючий втручається у взаємодію між відправником і одержувачем і може модифікувати трафік, переданий між ними. Тому відкритий ключ одержувача "підписується" ЦСК. Це означає, що ЦСК використовує свій секретний ключ для захисту відкритого ключа адресата. Оскільки тільки ЦСК знає свій секретний ключ, це є певною гарантією того, що відкритий ключ адресата отриманий саме від ЦСК.

5. Після одержання відправником відкритого ключа адресата він перевіряє його за допомогою відкритого ключа ЦСК і асиметричного криптоалгоритму. При цьому, природно, припускається, що ЦСК не був скомпрометований. Якщо ж він виявляється скомпрометованим, то це виводить із ладу всю мережу його користувачів.

6. Далі відправник шифрує сеансовий ключ з використанням асиметричного криптоалгоритму й відкритого ключа одержувача (отриманого від ЦСК і розшифрованого). Оскільки зашифрований сеансовий ключ передається по незахищеній мережі, він є очевидним об'єктом різних атак. Але його безпека гарантується стійкістю асиметричного криптоалгоритму та безпекою секретного ключу отримувача.

7. Зашифрований сеансовий ключ поєднується із шифротекстом, що включає додану раніше ЕЦП.

8. Увесь отриманий пакет даних, а саме, зашифрований сеансовий ключ і шифротекст, який крім вихідного тексту включає його ЕЦП, передається адресату.

9. Адресат виділяє з отриманого пакета зашифрований сеансовий ключ, який розшифровує використовуючи свій секретний ключ і той же самий асиметричний криптоалгоритм шифрування.

10. Потім, адресат, застосовуючи той же самий симетричний криптоалгоритм і розшифрований сеансовий ключ, відновлює із шифротекста

вихідний текст разом з ЕЦП. Електронний підпис відокремлюється від вихідного тексту.

11. Адресат запитує в ЦСК відкритий ключ ЕЦП адресанта. Після одержання цього ключа, адресат розшифровує його за допомогою відкритого ключа ЦСК і відповідного асиметричного криптоалгоритма.

12. Потім розшифровується хеш-функція тексту з використанням відкритого ключа адресанта й алгоритму ЕЦП і обчислюється хеш-функція отриманого розшифрованого тексту. Дві ці хеш-функції рівняються для перевірки того, що текст не був змінений. У випадку їх збігу підтверджується справжність повідомлення.

Порядок забезпечення криптографічного захисту інформації

Існуюча нормативно-правова база визначає, що для захисту конфіденційної інформації використовуються сертифіковані засоби КЗІ. Захист інформації з обмеженим доступом що є власністю держави, здійснюється за допомогою засобів, що мають допуск до експлуатації.

Проведення сертифікації засобів КЗІ та роботи із допуску до експлуатації (експертизи в сфері КЗІ) організує ДержспецзвязокУкраїни, що акредитований в Український Системі сертифікації продукції (УкрСЕПРО) як орган сертифікації засобів захисту інформації. На основу проведених робіт цей державний орган видає сертифікати та експертні висновки.

Організація й проведення сертифікації ЗКЗІ регламентуються нормативними документами системи УкрСЕПРО. Сертифікація ЗКЗІ здійснюється з метою підтвердження їх відповідності державним стандартам (зокрема, ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95) і іншим нормативним документам і технічним умовам на ці засоби. Процедури сертифікації є відкритими й загальнодоступними.

Експертиза в сфері КЗІ проводиться згідно з Положенням про державну експертизу в сфері криптографічного захисту інформації.

Процедури допуску до експлуатації (експертизи) і сертифікації багато в чому дуже схожі, разом з тим вони мають і ряд відмінностей.

Перелік об'єктів допуску до експлуатації (експертизи) значно ширше, чим у процедурі сертифікації. На відміну від сертифікації, об'єктами експертизи крім засобів КЗІ можуть бути:

- засоби й методи, призначені для розробки, дослідження, виробництва й випробувань засобів ЗКЗІ;
- звіти про наукові дослідження й розробках, інші результати наукової й науково-технічної діяльності в сфері КЗІ;
- криптографічні алгоритми й протоколи, методи генерації ключової інформації;
- криптографічні системи, засоби й устаткування КЗІ;
- положення програм і проектів державного значення в частині, що стосується КЗІ;
- системи й засоби генерації, тестування й розподілу ключів.

У такий спосіб сфера застосування експертизи ширше, чим сертифікації. Зокрема, експертиза в сфері КЗІ надає можливість у тому або іншому випадку

визначити можливість використання для захисту інформації конкретного криптоалгоритму й надати рекомендації щодо його застосування.

Вибір криптоалгоритми для захисту ІзОД є вельми чутливим етапом. Вже було зазначено раніше, що безпека інформації, що захищається за допомогою засобів КЗІ за умови забезпечення таємності ключа цілком і повністю залежить від криптографічної стійкості застосованих алгоритмів.

Криптоалгоритми засобів КЗІ, що призначені для захисту інформації з обмеженим доступом повинні бути державними стандартами або рекомендованими Держспецзв'язком України.

Віднесення криптоалгоритмів до переліку рекомендованих здійснюється в результаті проведення досліджень, оцінки криптографічних властивостей алгоритму і співвіднесення їх із сучасним рівнем розвитку науки й техніки. При цьому вивчається можливість реалізації певних загроз та необхідні для цього ресурси, включаючи обчислювальні потужності та вірогідність створення спеціалізованих пристроїв для реалізації визначених крипто аналітичних атак.

Одним з найбільш часто обговорюваних у зв'язку з криптографічними алгоритмами є питання довжини їх ключа. Можна почути різні думки з цього приводу. Зокрема, ряд авторів відносить питання довжини ключа алгоритму до другорядних, аргументуючи це тім фактом, що найбільший збиток криптосистемам наносять помили їх проектування.

Слід зазначити, що рівень криптографічної стійкості алгоритму при його правильній розробці суттєво залежить від довжини використовуваних ключів, а точніше - кількості різних припустимих варіантів ключів. Із зростанням довжини ключу в загальному випадку збільшується кількість варіантів ключу, що зменшує ймовірність їх розкриття аналітичним шляхом або завдяки їх підбору за допомогою потужних комп'ютерів.

Вартість засобів захисту в значній мірі визначається власне інформацією, яка захищається. Для захисту комерційної конфіденційної інформації природно використовувати засоби, вартість яких адекватна вартості інформації, що захищається. Інформація з обмеженим доступом, що є власністю держави вимагає «індивідуального» підходу в кожному конкретному випадку.

Основними перевагами апаратних засобів КЗІ насамперед є:

- висока продуктивність (швидкість обробки);
- безпека застосування завдяки реалізації апаратних схем контролю правильності функціонування (само тестування) і блокування роботи у випадку виявлення несправностей та помилок операторів;
- висока надійність (наробіток на відмову), збереження працездатності в широкому діапазоні температур, стійкість до несприятливих впливів навколишнього середовища (вологість, роса), можливість експлуатації на мобільних об'єктах з живленням від бортової мережі, відносно мала вага;
- можливість забезпечення в необхідних випадках ефективного захисту від витоку інформації за рахунок технічних каналів;
- можливість створення ефективної системи блокувань від несанкціонованого доступу до інформації й сигналізації;

- зручність підключення термінального і канального обладнання, сумісність по габаритах з типовими комунікаційними стійками;

- можливість функціонувати тривалий час у встановлених умовах;

- досить високий рівень захищеності критичної інформації в обладнанні (у т.ч. алгоритму, секретних параметрів).

Разом з тим, як уже було відзначено, відносно висока вартість апаратних засобів КЗІ й неможливість досить швидко змінювати сервісні функції є основними їхніми недоліками.

Програмні засоби КЗІ створюються, як правило, на основі універсальних (загального призначення) комп'ютерів і разом з універсальністю несуть відбиток усіх їхніх переваг і недоліків у плані захисту від реальних загроз.

Зокрема, виграш у вартості програмних засобів в порівнянні з апаратними відчутний тільки доти, поки не враховується фактор можливості послаблення безпеки комп’ютерної системи за рахунок наявності технічних каналів витоку інформації (наприклад, радіоканалів). Після реалізації необхідних заходів із технічного захисту комп’ютеру застосування спеціалізованих засобів може виявитися навіть дешевшим.

Програмні засоби також можуть не забезпечувати необхідну швидкодію, наприклад, коли потрібно мати пропускну здатність на рівні декількох мегабіт за секунду.

Залишимо можливість користувачам самим на основі викладених підходів проводити порівняльний аналіз конкретних апаратних та програмні засобів КЗІ.

Залежно від характеру передачі інформації в канал застосовують два основні види шифрування: попереднє й лінійне.

У першому випадку вихідне повідомлення попередньо зашифровується, після чого воно передається в канал. Цей вид переважно використовується для захисту даних в системах електронної пошти

У другому варіанті засіб КЗІ працює синхронно з каналом і кожний зашифрований символ повідомлення негайно передається в канал (лінію).

Зовні невелика відмінність висуває істотні додаткові вимоги до засобу КЗІ, що реалізує лінійне шифрування. Насамперед це стосується системи синхронізації, що забезпечує спільну роботу двох шифраторів.

Шифрування повідомлень в захищених телекомунікаційних системах здійснюється за допомогою двох основних способів:

- «лінія за лінією» коли повідомлення в зашифрованому вигляді перебуває тільки між двома сусідніми вузлами мережі (абонентом і комутаційним вузлом, двома комутаційними вузлами). Цей спосіб шифрування застосовується на високошвидкісних каналах зв'язку (від 2,048 Мб/сек) між двома вузлами комутації, коли завдяки мультиплексуванню (об’єднанню) шифрується впорядкована суміш даних багатьох абонентів;

- «від кінця до кінця» або абонентське шифрування, за умов якого захист трафіку здійснюється на протязі з'єднання (іноді віртуального) двох абонентів. На відміну від першого способу в цьому варіанті забезпечується захист даних у тому числі на вузлах комутації. Проблема впровадження даного способу

полягає у високій вартості повно зв'язаної (кожний має зв'язок з кожним) системи.

На практиці виходячи з економічних міркувань, доцільності й умов безпеки зв'язку використовують комбінацію способів «лінія за лінією» і абонентського шифрування.

Засоби КЗІ, що реалізують останній спосіб шифрування, називають ще абонентськими засобами шифрування.

Проектування схеми захищеному зв'язку, як правило, здійснюється одночасно з розробкою схеми телекомунікаційної складової системи. В іншому випадку, зазвичай, роботи із захисту складніше й коштують вони суттєво дорожче.

На етапі проектування повинна бути визначена потреба захищеної системи в наступних елементах:

- швидкісних засобах шифрування, що забезпечують захищений трафік для основної маси абонентів;

- стаціонарних абонентських ЗКЗІ, що застосовуються для користувачів високого рангу або абонентів, офіси яких перебувають за межами контрольованих зон;

- мобільних абонентських ЗКЗІ;

- стаціонарних засобах попереднього шифрування;

- системах (центрах) генерації й розподілу ключових даних.

Велика кількість абонентів і типів апаратури майже обов'язково зажадає розв'язки проблеми зв'язаності мережі в змісті можливості забезпечити з'єднання абонента з одним типом обладнання (набором ключів) з абонентом, що мають у своєму розпорядженні інший тип обладнання (і, відповідно, інший набір ключів).

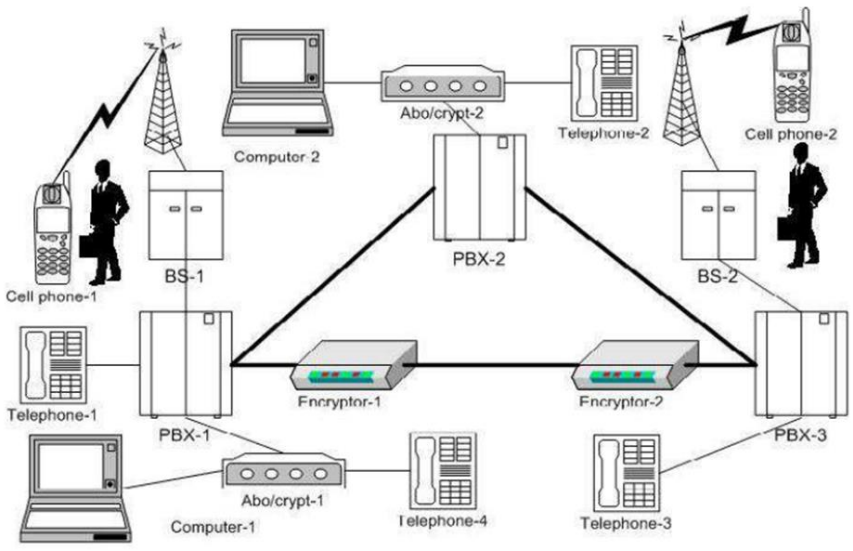


Рис. 8.4. Варіант схеми побудови системи захищеного зв’язку

На рис.8.4 представлений спрощений варіант схеми захищеному зв'язку.

На схемі показані основні принципи забезпечення безпеки інформації:

- комутаційні станції РВХ-1 і РВХ-3 двох офісів з'єднані за допомогою шифраторів Encryptor-1 і Encryptor-2, що забезпечують обмін із необхідною швидкістю. При цьому, абоненти Telephon-1 і Telephon-3, що перебувають на

контрольованій території, мають можливість вести переговори в захищеному режимі;

- комутаційні стації PBX-1 і PBX-2 з'єднані по відкритих каналах, тому для забезпечення зв'язку в захищеному режимі абонентів Computer-1, Telephon-1 – з одного боку, і Computer-1 Telephon-2 – з іншого боку, здійснюють обмін через абонентські шифратори Abo/crypt-1 і Abo/crypt-2;

- для забезпечення мобільного зв'язку абонентів криптотелефонів Cellphone-1 і Cellphone-2 комутаційні станції PBX-1 і PBX-3 мають вихід на базові станції мобільного зв'язку BS-1 і BS-2 (можливо, варіант у стандарті стільникового зв'язку GSM або CDMA). Зазначимо, що в цьому варіанті на ділянці між станціями PBX-1 і PBX-3 повідомлення абонентів Cellphone-1 і Cellphone-2 передаються у двічі зашифрованому виді;

- замість багатофункціональних абонентських шифраторів Abo/crypt-1,2 для забезпечення роботи тільки в режимі електронної пошти можуть використовуватися апаратно-програмні ЗКЗІ, у яких шифрування інформації реалізується за допомогою апаратного пристрою, наприклад, з USB інтерфейсом.

У цей час рядом вітчизняних компаній розробників і виробників створені сучасні апаратні шифратори, що дозволяють надійно захищати конфіденційну інформацію (табл. 3). Ряд виробів уже пройшли експертизу й одержали необхідні документи від Держспецзв'язку України, деякі перебувають у процесі експертизи.

Таблиця 3 – Шифратори потокового типу для захисту конфіденційної інформації

№№ п.п.	Умовне найменування	Тип	Характеристика	Заявлена швидкість	Фірма
1.	«CryptoIP-448»	АШ,КШ, ЕЦП	TCP/IP, IEEE 802.3, НК - смарткарта	6 Мб/	А
2.	«CryptoIP-248»	АШ,КШ, ЕЦП	TCP/IP, IEEE 802.3, НК - смарткарта	1 Мб/	А
3.	«Онікс-100»	КШ	TCP/IP, IEEE 802.3, НК - МКД	75 Мб/	К
4	Д-300	КШ	E1, ITU-T G.703, G.704, G.706, НК - МКД	2048 Кб/з	К
5.	«Пелена» В 371-Е	КШ	TCP/IP, Ethernet.IEEE 802.3-2002 100Base-tx/FX, НК – ISO 7816	70 Мб/з	Т
6.	В 271-Е	АШ	TCP/IP, 4 Ethernet 100 Base-sx, НК – ISO 7816	30 Мб/з	Т

Скорочення, абревіатури:

АШ – абонентське шифрування, КШ – канальне шифрування, ЕЦП – формування електронного цифрового підпису, TCP/IP – стік протоколів, E1 – основний потік зі швидкістю 2048 кб/сек, «А» - ТОВ «Автор», «К» - ТОВ «НВФ «Криптон», «Т» - ТОВ «Трител».

ТЕМА 8. Інженерно-технічні методи убезпечення об’єктів інформаційної діяльності

Забезпечення безпеки інформації потребує застосування різних методів захисту, які не суперечать та взаємно доповнюють один другого. У цьому випадку можливо стверджувати про досягнення необхідних та достатніх умов надійного захисту інформації.

В основі створення системи захисту інформації полягає принцип багаторівневого її убезпечення, тобто принцип послідовних кордонів, що дозволяють своєчасно виявити потенційні загрози та побудувати перешкоди на шляху поширення загроз.

Вказані кордони обмежують так звані зони безпеки, що розташовуються послідовно від зовнішньої огорожі навколо об’єкту інформаційної діяльності безпосередньо до приміщень, у яких обробляється інформація, що захищається.

Для побудови зон безпеки застосовуються паркани навколо території, засоби обмеження доступу до будівель та споруд, спеціально обладнані під’їзди та проходи (шлагбауми, турнікети), ролети або грати на вікнах та вентиляційних отворах, засоби освітлення у нічний час, системи сигналізації та відео спостереження.

Таким чином, можливо говорити, що важливими складовими безпеки об’єктів інформаційної діяльності є фізичний та інженерно-технічний захист.

Фізичний захист забезпечується службою охорони, основним завданням якої є попередження несанкціонованого фізичного проникнення порушників на контрольовану територію та стримування їх до прибуття сил правопорядку.

Інженерно-технічний захист передбачає використання посилених дверей, металевих грат та огорож, надійних замків та сейфів.

Також цей вид захисту передбачає застосування методів та засобів охоронної сигналізації, відео спостереження, засобів спецзв’язку, резервного електроживлення та освітлення.

Методи й засоби контролю, сигналізації, розмежування доступу на об'єкти інформаційної діяльності

Для захисту об'єктів та інформаційних ресурсів від загроз традиційного шпигунства й диверсій, як було зазначено раніше, повинні бути вирішені наступні завдання: Для захисту об'єктів та інформаційних ресурсів від загроз традиційного шпигунства й диверсій, як було зазначено раніше, повинні бути вирішені наступні завдання:

- створення системи охорони об'єкта;
- організація робіт з конфіденційними інформаційними ресурсами на об'єкті;
- протидія спостереженню;
- протидія підслуховуванню;
- захист від злочинних дій персоналу.

Об'єкт, на якому проводяться роботи з цінною інформацією, має, як правило, кілька рубежів захисту:

- контрольована територія;

- будинок:
- приміщення;
- пристрій, носій інформації;
- програма;
- інформаційні ресурси.

Від шпигунства й диверсій необхідно охороняти перші чотири рубежі й обслуговуючий персонал.

Система охорони об'єкту (СОО) створюється з метою запобігання несанкціонованого проникнення на територію й у приміщення об'єкта сторонніх осіб, що обслуговує персонал й користувачів.

Склад системи охорони залежить від охоронюваного об'єкту. У загальному випадку СОО повинна включати наступні компоненти:

- інженерні конструкції;
- охоронна сигналізація;
- засоби спостереження:
- підсистема доступу на об'єкт;
- чергова зміна охорони.

Інженерні конструкції служать для створення механічних перешкод на шляху зловмисників. Вони створюються по периметру контрольованої зони. Інженерними конструкціями обладнуються також будинки й приміщення об'єктів. По периметру контрольованої території використовуються бетонні або цегельні забори, ґрати або сіткові конструкції.

Для підвищення захисних властивостей загороджень поверх заборів зміцнюється колючий дріт, гострі стрижні, армована колюча стрічка. Остання виготовляється шляхом армування колючої стрічки сталевим оцинкованим дротом діаметром 2,5 мм. Армована колюча стрічка часто використовується у вигляді спіралі діаметром 500…955 мм.

Для утруднення проникнення зловмисника на контрольовану територію можуть використовуватися малопомітні перешкоди. Прикладом малопомітних перешкод може служити металева мережа з тонкого дроту. Така мережа розташовується уздовж забору на ширину до 10 метрів. Вона виключає швидке переміщення зловмисника.

У будинки й приміщення зловмисники намагаються проникнути, як правило, через двері або вікна. Тому за допомогою інженерних конструкцій їх зміцнюють,оскільки це слабка ланка в захисті об'єктів. Надійність дверей залежить від механічної міцності самих дверей і від надійності замків. Вимоги до механічної міцності й здатності протистояти несанкціонованому відкриванню пред'являються до замка.

Замість механічних замків усе частіше використовуються кодові замки. Найпоширенішими серед них (називаних звичайно сейфовими замками) є дискові кодові замки із числом комбінацій коду ключа в межах $10^6 \ldots 10^7$.

Найвищу стійкість мають електронні замки, побудовані із застосуванням мікросхем. На базі електронних замків будуються автоматизовані системи контролю доступу в приміщення.

У кожний замок уводяться номери мікросхем, власники яких допущені у відповідне приміщення. Може також задаватися індивідуальний часовий інтервал, протягом якого можливий доступ у приміщення. Усі замки можуть поєднуватися в єдину автоматизовану систему, центральною частиною якої є автоматизоване робоче місце адміністратора безпеки.

За статистикою понад 80% випадків проникнення на об'єкти відбувається через віконні отвори. Ці дані свідчать про необхідність інженерного зміцнення вікон, яке здійснюється двома шляхами:

- установка віконних грати;
- застосування стекол, стійких до механічного впливу.

Охоронна сигналізація служить для виявлення спроб несанкціонованого проникнення на охоронюваний об'єкт.

Системи охоронної сигналізації повинні відповідати наступним вимогам:

- охоплення контрольованої зони по всьому периметру;
- висока чутливість до дій зловмисника;
- надійна робота в будь-яких погодних і часових умовах;
- стабільність до природних перешкод;
- швидкість і точність визначення місця порушення;
- можливість централізованого контролю подій.

Охоронна система являє собою систему датчиків (джерело тривоги), об'єднаних шлейфом сигналізації для подачі сигналів на приймальноконтрольний пристрій, який видає сигнал тривоги на оповіщувач.

Датчик являє собою пристрій, що формує електричний сигнал тривоги при впливі на датчик або на створюване їм поле зовнішніх сил або об'єктів.

Шлейф сигналізації утворює електричне коло для передачі сигналу тривоги від датчика до приймально-контрольного пристрою.

Приймально-контрольний пристрій служить для приймання сигналів від датчику їхньої обробки й реєстрації, а також для видачі сигналів в оповіщувач.

Оповіщувач видає світлові й звукові сигнали черговому охоронцеві.

За принципом виявлення зловмисників датчики діляться на:

- контактні;
- акустичні;
- електронні, оптико-електронні;
- мікрохвильові;
- вібраційні;
- ємнісні;
- телевізійні.

Організація безперервного спостереження або відеоконтролю за об'єктом є однієї з основних складових системи охорони об'єкта.

У сучасних умовах функція спостереження за об'єктом реалізується за допомогою систем телебачення. Їх називають також телевізійними системами відеоконтролю (ТСВ).

Телевізійна система відеоконтролю забезпечує:

- автоматизоване відеоспостереження за рубежами захисту;
- контроль над діями персоналу організації;

- контроль над діями персоналу організації;
- відеозапис дій зловмисників;
- режим відеоохорони.

У режимі відеоохорони ТСВ виконує функції охоронної сигналізації. Оператор ТСВ сповіщається про рух у зоні спостереження. У загальному випадку телевізійна система відеоконтролю включає наступні пристрої:

- передавальні телевізійні камери;
- монітори;
- пристрій обробки й комутації відеоінформації;
- пристрої реєстрації інформації.

Доступ на об'єкти проводиться на контрольно-пропускних пунктах (КПП), прохідних, через контрольований вхід у будинки й приміщення. На КПП і прохідних чергують контролери зі складу чергової зміни охорони.

Вхід у будинки й приміщення може контролюватися тільки технічними засобами. Прохідні, КПП, входи в будинки й приміщення обладнаються засобами автоматизації й контролю доступу.

Одним з основних завдань, розв'язуваних при організації допуску на об'єкт, є ідентифікація й автентифікація осіб, що допускаються на об'єкт. Їх називають суб'єктами доступу.

Під ідентифікацією розуміється присвоєння суб'єктам доступу ідентифікаторів і (або) порівняння пропонованих ідентифікаторів з переліком привласнених ідентифікаторів, власники (носії) яких допущені на об'єкт.

Автентифікація означає перевірку приналежності, суб'єктові доступу пред'явленого їм ідентифікатора, підтвердження справжності.

Розрізняють два способи ідентифікації людей: атрибутивний і біометричний. Атрибутивний спосіб припускає видачу суб'єктові доступу або унікального предмета, або пароля (коду), або носія (смарткарта, токен), що містить код.

Предметами, що ідентифікують суб'єкт доступу, можуть бути звичайні пропуски, жетони або ключі від вхідних дверей (кришок пристроїв), а також різного виду картки.

Усі атрибутивні ідентифікатори мають один істотний недолік. Ідентифікаційна ознака слабко або зовсім не пов'язаний з особистістю пред'явника.

Цього недоліку позбавлені методи біометричної ідентифікації. Вони засновані на використанні індивідуальних біологічних особливостей людини.

Для біометричної ідентифікації людини використовуються його унікальні особливості, як то:

- папілярні візерунки пальців;
- візерунки сітківки ока;
- особливості мови;
- форма й розміри особи;
- динаміка підпису й ін.

Основною перевагою біометричних методів ідентифікації є достатньо висока ймовірність виявлення спроб несанкціонованого доступу.

доступі суб'єктові, що має право на доступ, становить майже 1%. Витрати на забезпечення біометричних методів доступу, як правило, перевершують витрати на організацію атрибутивних методів доступу.

Для підвищення надійності автентифікації використовуються кілька ідентифікаторів.

Підсистема доступу на об'єкт виконує також функції реєстрації суб'єктів доступу й керування доступом.

Склад чергової зміни, його екіпірування, місце розміщення визначається статусом охоронюваного об'єкта. Використовуючи охоронну сигналізація, системи спостереження й автоматизації доступу, чергова зміна охорони забезпечує тільки санкціонований доступ на об'єкт і в охоронювані приміщення.

Чергова зміна може перебувати на об'єкті постійно або прибувати на об'єкт при одержанні сигналів тривоги від систем сигналізації й спостереження.

Спостереження за деяким об'єктом (зловмисником), що перебуває на значному віддаленні, в оптичному діапазоні, малоефективне. З відстані 50 м навіть за допомогою довгофокусного фотооб'єктива без стаціонарної системи спостереження практично неможливо прочитати текст із документа або монітора. Крім того, загрози такого типу легко нейтралізуються за допомогою:

- застосування штор і захисного фарбування скла;
- використання шибок з однобічною провідністю світла;
- розміщення робочих столів, моніторів, табло й плакатів таким чином, щоб вони не проглядалися через вікна або відкриті двері.

Для протидії спостереженню в оптичному діапазоні зловмисником, що перебувають на об'єкті, необхідно, щоб:

- двері приміщень були закритими;
- розташування столів і моніторів ЕОМ виключало можливість спостереження документів або видаваної інформації на сусідньому столі або моніторі;
- стенди з конфіденційною інформацією мали штори.

Методи мінімізації збитків від аварій і стихійних лих

Стихійні лиха й аварії можуть завдати величезної шкоди об'єктам автоматизованих систем, у тому числі, у плані втрати коштовної інформації або створення передумов для її витоку.

Повністю запобігти стихійним лихам у більшості випадків не під силу жодній державі, але зменшити негативні наслідки таких явищ у багатьох випадках вдається навіть у масштабах щодо невеликих підприємств. Мінімізація наслідків аварій і стихійних лих для об'єктів інформаційних систем може бути досягнута шляхом:

- правильного вибору місця розташування об'єкта;
- обліку найбільш імовірних аварій і стихійних лих при розробці й експлуатації системи;
- організації своєчасного оповіщення про можливі стихійні лиха;
- навчання персоналу діям під час стихійних лих і аварій, а також методам ліквідації їх наслідків.

Об'єкти інформаційних систем по можливості повинні розташовуватися в тих районах, де не спостерігається таких стихійних лих як повені, землетруси. Об'єкти необхідно розміщати вдалечині від таких небезпечних об'єктів як хімічні підприємство з виробництва небезпечних реагентів, нафтобази й нафтопереробні заводи, склади горючих і вибухових речовин, греблі і т.д.

На практиці далеко не завжди вдається розташувати об'єкт на достатньому віддаленні від небезпечних підприємств або районів з можливими стихійними лихами. Тому при розробці, створенні й експлуатації об'єктів інформаційних систем необхідно передбачити спеціальні заходи.

У районах з можливими землетрусами (Крим, Карпати) будинки повинні бути сейсмостійкими. У районах можливих затоплень основне обладнання доцільно розміщати на верхніх поверхах будинків. Усі об'єкти повинні забезпечуватися автоматичними системами гасіння пожежі.

На об'єктах, для яких імовірність стихійних лих висока, необхідно здійснювати розподілене дублювання інформації й передбачити можливість перерозподілу функцій об'єктів.

На всіх об'єктах повинні передбачатися заходи на випадок аварії в системах електроживлення. Для об'єктів, що працюють із коштовною інформацією, потрібно мати аварійні джерела безперебійного живлення й підведення електроенергії провадити не менш ніж від двох незалежних ліній електроживлення.

Використання джерел безперебійного живлення забезпечує, принаймні, завершення обчислювального процесу й збереження даних на зовнішніх запам'ятовувальних пристроях.

Втрати інформаційних ресурсів можуть бути суттєво зменшені, якщо обслуговуючий персонал буде вчасно попереджений про природні катаклізми, що насуваються. У реальних умовах така інформація часто не встигає дійти до виконавців. Тому персонал повинен бути навчений діям в умовах стихійних лих і аварій, а також уміти відновлювати втрачену інформацію.

Методи та моделі стеганографії

Стеганографія - у перекладі з грецької мови («steganos» - «таємний», «graphos» - «пишу»), означає «тайнопис». Це наука про приховану передачу інформації та збереження у таємниці власне факту її передавання. На відміну від криптографії, яка змінює зміст таємного повідомлення, стеганографія приховує факт існування таємної інформації або каналу передавання.

Таким чином, стеганографія, як наука, досліджує та розробляє методи інформаційного обміну, у разі застосування яких приховується факт існування спеціального (секретного) зв'язку. Вона не підмінює технології технічного або криптографічного (шифрування) захисту даних, а лише доповнює їх ще одним рівнем безпеки.

Під час оброблення даних стеганографічними методами відбувається приховування інформації, яка передається, в деяких масивах іншої інформації (аудіо та відео файли, статичні малюнки великого розміру) так, щоб стороння особа навіть не здогадувалася про існування прихованого таємного повідомлення. При цьому виявити таке повідомлення доволі складно, а якщо

додатково застосовується надійне зашифрування порушник не зможе з’ясувати зміст повідомлення, навіть у випадку його виявлення.

Вперше про стеганографію згадується ще у 5-ому сторіччі до н.е. Літописи Геродоту донесли до нас цікаву історію. Тиран Гистий, захоплений перськими військами у грецьких Сузах, захотів надіслати листа своєму родичу у Мілієт, що в Анатолії. Для цього він наказав поголити наголо раба та на його голові у вигляді тату відобразити план розміщення військ персів. Після того, як волосся знову виросло, раб доставив повідомлення.

Методи стеганографії застосовувалися російськими революціонерами у листах з тюрем. Це були повідомлення, що написані молоком між рядків зовнішньо звичайного листа. Таємний текст з'являвся, якщо папір нагрівався за допомогою гарячої праски або свічки. Також застосовувалися з аналогічною метою різні хімічні речовини.

За часів другої світової війни німецькі спеціальні служби активно застосовували так звані мікрокрапки - мікроскопічні фотознімки, що вклеювалися у тексти листів, документів.

З часом, з впровадженням науково-технічних досягнень у повсякденне життя, елементи стеганографії почали з’являтися в телеграфних повідомленнях, радіограмах, потім, на носіях цифрової інформації.

У поточний час стеганографія все частіше асоціюється з приховуванням інформації у графічних або текстових файлах комп'ютерних систем за допомогою спеціального програмного забезпечення.

Комп'ютерна і цифрова стеганографія, цифрові водяні знаки

Розрізняють декілька напрямів стеганографії, що сформувалися наприкінці 90-х років минулого сторіччя - часу, що вважається її другім народженням.

Класична стеганографія включає наступні напрями:

- комп'ютерна стеганографія - розділ класичної стеганографії, методи якого спеціально розроблені для застосування у комп'ютерних системах. Наприклад, стеганографічна файлова система StegFS, що працює у середовищі операційної системи Linux, забезпечує приховування даних у невикористаних областях форматів файлів.

- цифрова стеганографія - напрям комп'ютерної стеганографії, що базується на приховуванні інформації в цифрових об’єктах, які спочатку мали аналогове походження. Це переважно мультімедійні об’єкти (статичні зображення, відео, аудіо).

Методи цифрової стеганографії забезпечують рівномірне розташування бітів одного типу інформації в іншій. При цьому приховування реалізується таким чином, щоб, під час відповідної модифікації вихідної інформації, не були втрачені її основні властивості - змістовність, цінність, достовірність.

Крім того, необхідно, щоб зовнішні характеристики новостворюваного інформаційного масиву не давали можливості виявляти факт передачі одного повідомлення у середині іншого методами аудіо та візуальної перевірки (тобто шляхом прослуховування або перегляду).

У якості носія інформації, що приховується, може застосовуватися іншій інформаційний об'єкт (файл), що припускає викривлення частини власного вмісту, внаслідок чого не порушується його функціональність. Тобто аудіофайл має прослуховуватися усіма встановленими для даного типу файлів кодеками (програвачами), теж саме відноситься до відео файлів та файлів зображень. Обсяг внесених за рахунок файлу, що приховується, викривлень не може перевищувати поріг чутливості засобів розпізнавання.

Носій інформації, що приховується, називається стеганографічним контейнером або просто контейнером.

У якості контейнеру використовуються файли, що мають велику надлишковість, тобто характеризуються здатністю «бути впізнаними» в умовах завад та перешкод. Крім того, вони мають бути достатньо великими за розміром для розміщення простого або форматованого тексту. Таким вимогам за звичай відповідають файли зображень, відео і аудіо файли. Повідомлення, що приховується, може бути набором символів або зображенням у двійковому вигляді, відкритим або зашифрованим текстом.

У багатьох мультимедійних форматах є поля розширення, які можуть містити дані користувача або прописані нулями. У останньому випадку їх також можливо використовувати для заповнення деякою інформацією для приховування. Але цей спосіб досить небезпечний та не дозволяє розташувати у такому «контейнері» достатній обсяг даних.

Рішення проблеми полягає у використанні надлишковості інформації.

Вихідний аналоговий сигнал (аудіо або зображення) містить надзвичайно великий обсяг інформації, який обмежується під час оцифровування. Тому у разі помірної зміни цифрових даних звичайна людина внаслідок особливостей слуху та зору не може помітити різницю між вихідною та модифікованою інформацією.

Зокрема, користуючись наявністю у молодших бітах зображень та інших мультимедійних файлів так званих випадкових шумів квантування, що розміщені рівномірно по всьому файлу, можливо побудувати деяку стеганографічну систему.

У якості контейнеру у цьому випадку візьмемо зображення у графіці середнього розрізняння розміром 800x600 точок – пікселів.

Кольоровий тон пікселю передається комбінацією трьох основних кольорів: червоного, зеленого і синього, кожен з яких кодується одним байтом, тобто для передачі пікселю використовується 3 байта або 24-біта. Загалом обсяг зображення сягає майже півтора мегабайта: 800x600x3=1 440 000 байт.

В стеганографічній системі кодування найменшого значущого біту (Least Significant Bits – LSB) кожного байта в цілому для приховування інформації використовується 3 біта на кожен піксель. Тому у контейнері максимально можливо розташувати $1.44x10_6$ біт вихідного повідомлення.

Якщо використовувати кожен молодший біт, то виявити цей факт за допомогою відповідних комп'ютерних програм досить легко. Тому необхідно випадково рівномірно «розсипати» біти повідомлення, що приховується, по припустимим місцям, таким чином, щоб порушник безпеки стеганографічної

системи не зміг зрозуміти: чи належить черговий біт контейнерові або повідомленню, яке відновлюється.

Для цього побудуємо стеганографічну систему наступним чином. Нехай M={mi , i=1,N} - вихідне повідомлення довжини N, множина {Pi , i=1÷1.44x10_6 } – послідовність молодших біт пікселів контейнеру, а {ki} – послідовність біт деякого ключу, що містить не менш N одиниць (N на багато менш ніж 1.44x10_6).

В цих позначеннях рівняння утворення модифікованої послідовності молодших біт контейнеру {Bi} записується у наступному вигляді:

$$B_i = P_i \cdot \bar{k}_i \oplus m_j \cdot k_i, \partial e\ j = \sum_{l=1}^{i-1} k_l,\ k_0 = 0,\ i = \overline{1,1.44 \cdot 10^6} \qquad (10.1)$$

Як можливо побачити з рівняння, у випадку значення чергового біта ключу $k_i = 1$ його інвертоване значення $k_i = 0$, внаслідок чого молодший біт пікселю контейнеру отримує значення чергового біту повідомлення що приховується $B_i = m_j$.

Коли маємо значення чергового біта ключу $k_i=0$ його інвертоване значення $k_i = 1$, тому значення молодшого біту пікселю контейнеру не змінюється $B_i = P_i$.

Замість довгої ключової послідовності в рівнянні (10.1) для вбудовування інформаційного повідомлення у контейнер можливо використовувати послідовності, що формуються за допомогою стійких алгоритмів шифрування.

Біти нової послідовності на деяких позиціях будуть співпадати з бітами контейнера (зображення, звук), в інших ні, але при цьому для невеликої порівняно с контейнером довжини вихідного повідомлення акустично або візуально виявити наявність таких спотворень практично не можливо.

За умов правильної генерації ключа, задача виділення вихідного повідомлення в стеганографічній системі LSB у випадку застосування схеми перетворення, що задається рівнянням (10.1), становиться вельми складною.

Прихованість каналу передачі та ступінь схожості з оригіналом підвищуються, якщо контейнер є файлом з оцифрованою фотографією або відсканованим зображенням за рахунок наявності шумів квантування у молодших розрядах байт. Випадковий шум у зображенні додатково маскує наявність у контейнері прихованої інформації.

Приклад результатів відповідного перетворення – вбудовування інформаційного повідомлення у контейнер, що є кольоровим зображенням, наведено на рис. 10.1.

Крім прихованої передачі повідомлень, стеганографічні перетворення є одним з перспективних методів, що використовуються для ідентифікації та маркування авторських виробів та боротьби з контрафактною продукцією (підробками).

Рис. 10.1 Результат стеганографічних перетворень

При цьому у якості ідентифікаційної інформації, що вбудована у деякій контейнер, застосовуються наступні дані: дата и місце створення продукту, відомості про автора (розробника, виробника), номер ліцензії, серійний номер виробу, дата завершення терміну дії придатності. Остання інформація є корисною при контролі розповсюдження умовно безкоштовних програм (англ. shareware).

Відповідна інформація за звичай впроваджується не тільки програмні продукти, а й у графічні, аудіо та відео твори. Усі включені відомості можуть розглядатися у суді як вагомі докази під час розгляду справ про авторські права для доведення фактів нелегального копіювання.

Модель комп'ютерної стеганографічної системи

Модель комп'ютерної стеганографічної системи (КСС) може бути умовно подана, як відображено на рис. 10.2.

З боку абонента А є деяка множина файлів-носіїв – контейнерів, які за суттю є оцифрованими фотографіями або аудіофайлами, а також власне файли - повідомлення, що підлягають передачі.

За допомогою деякого стеганографічного алгоритму і ключів (можливо одного фіксованого для всіх повідомлень) здійснюється вбудовування в контейнери вихідних повідомлень. Потім файл передається абоненту Б, якій знає алгоритм та за допомогою ключу вилучає з контейнеру інформацію, що передана.

Для підвищення надійності приховування каналу передачі в КСС може використовуватися відправлення «пустих» контейнерів, що не містять інформаційних повідомлень. Підвищенню конфіденційності інформації, яка передається, сприяє попереднє шифрування файлів.

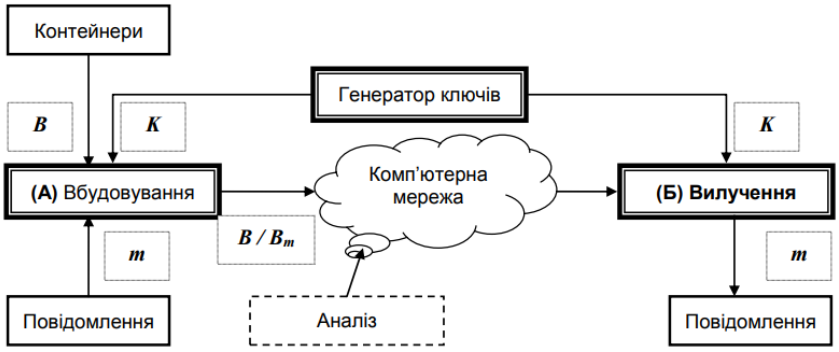


Рис. 10.2. Модель комп'ютерної стеганографічної системи

У загальному випадку пряме і зворотне рівняння стеганографічного перетворення можливо записати у наступному вигляді:

$$b_{m,k} = F(m,b,k) \quad m = F^{-1} = (b_{m,k},k) \qquad (10.2)$$

де:

$m \in M$ (слід читати: m належить множині M) - деяке вихідне повідомлення з множини усіх можливих повідомлень;

$b, b_{m,k} \in B$ - відповідно: пустий та модифікований контейнери з множини припустимих контейнерів B. Модифікований контейнер $b_{m,k}$ називають стеганограмою;

$k \in K$ - припустимий стегоключ с множини усіх ключів.

Вважається, що порушник системи безпеки, за аналогією з випадком криптографічної системи, має на меті наступні задачі:

- виявлення факту прихованої передачі інформації;
- порушення конфіденційності - вилучення з файлів-контейнерів вихідних повідомлень;
- порушення доступності - знищення прихованої інформації;
- порушення цілісності - модифікація (підробка) переданого повідомлення, нав'язування неправдивої інформації.

Таким чином, КСС – система, що забезпечує створення прихованого каналу передачі (зберігання) інформації на основі відкритого каналу з використанням особливостей сприйняття людиною різних видів інформації (аудіо, відео, графічні зображення).

При цьому основними вимогами до КСС є максимальне ускладнення задач виявлення (компрометації) порушником прихованого каналу та вилучення/модифікація/знищення інформації із/в контейнерів(ах).

Вразливості стеганографічних систем

Методи стегоаналізу, як методологія атак на стеганографічні системи, переважно базуються на статистичних критеріях, які дозволяють виявити деякі неоднорідності, залежності (кореляції) та нерівномірності у послідовностях символів можливо модифікованих контейнерів, що обумовлені принципами побудови системи та статистичними властивостями відкритих повідомлень.

Слід мати на увазі, що стегосистема з постійним ключем є найбільш небезпечною і може знайти практичне застосування лише за умов невеликого обсягу інформаційного обміну або частої зміни контейнерів.

За аналогією з криптографією особу, що робить спроби розкрити КСС та виділити повідомлення називають стегоаналітиком.

Відповідно спробу виявити наявність повідомлення та встановити його зміст називають атакою на стеганографічну систему.

На відміну від криптографії під розкриттям КСС прийнято розуміти пошук такої її вразливості, яка дозволяє встановити факт приховування повідомлення у контейнері та довести цей факт третій стороні з високою вірогідністю.

З урахуванням викладеного, атаки на КСС можливо розділити на наступні види:

1. Атака зі знанням тільки стеганограми – аналог криптоаналітичної атаки зі знанням шифрованого тексту. Стегоаналітик у цьому випадку має лише можливо модифікований контейнер, за допомогою якого робить спробу встановити наявність прихованого повідомлення. Даний вид стеганографічної атаки є базовим для оцінки якості КСС.

2. Атака з відомим контейнером має місце у випадку, коли стегоаналітик має деяку кількість пар «контейнер – стеганограма». Порівняно з попередньою ситуацією відомий вихідний контейнер, що дає суттєві переваги для проведення аналізу.

3. Атака з вибраним контейнером передбачає можливість нав'язування інформації в КСС для конкретного виду контейнеру.

4. Атака с відомим повідомленням здійснюється в умовах, коли порушнику відомі декілька можливих варіантів повідомлень, та йому необхідно встановити факт їх передачі за допомогою КСС та відновити використаний ключ

Можливо підкреслити, що як і в випадку криптоаналізу, атаки можуть бути адаптивними, якщо стегоаналітик отримує доступ до вибору повідомлень або контейнерів залежно від отриманих раніше результатів.

Підсумовуючі викладене, можливо зробити висновок, що не зважаючи на певну нормативно-правову невизначеність питань застосування стеганографічного захисту, відповідні технології є ефективним інструментом для приховування каналів обміну таємною інформацією або підтвердження авторських прав.

ТЕМА 9. Методи відновлення та гарантованого знищення інформації

Оброблення інформації з обмеженим доступом з допомогою обчислювальної техніки потребує вирішення двох протилежних задач:

- гарантоване знищення даних на машинних носіях у необхідних випадках. При цьому мається на увазі таке знищення, внаслідок якого інформація з носія не може бути зчитана аніякім методом;
- відновлення інформації з машинних носів, на яких вона була пошкоджена внаслідок випадкових або навмисних дій.

Обидві проблеми мають складні фізико-технічні рішення, зупинимося на методах їх розв'язання детально. Матеріал цього розділу публікується з дозволу компанії «ЕПОС», яка є автором відповідних технологій, рішень та засобів.

Проблеми й технології відновлення доступу до даних, збережених на машинних носіях

Відновлення даних може бути необхідно у наступних випадках:

- фізичні пошкодження носіїв інформації (рис. 11.1), їх елементів, наприклад руйнування дисків (рис. 11.2), пошкодження блоку магнітних голівок;
- після видалення розділів і файлів (рис. 11.3);
- після логічного руйнування файлових систем (NTFS, FAT і ін.);
- після форматування дисків;
- електричні й механічні пошкодження елементів електроніки;
- поява збійних секторів («bad»-блоків) на поверхнях дисків або в чарунках пам'яті;
- руйнування службової інформації накопичувача.

Рис. 11.1 Комп'ютер, пошкоджений внаслідок пожежі

Причинами, внаслідок яких знищуються дані, можуть бути апаратні та, помилки користувачів, вплив вірусів, навмисні дії, пожежі та інші стихійні лиха. На рис. 11.1 показано комп'ютер, пошкоджений після пожежі, інформацію на якому повністю відновлено за технологією ТОВ «ЕПОС».

Для відновлення інформації використовується спеціалізоване устаткування й програмне забезпечення.

У поточний час відпрацьовані методи та технології відновлення інформації на наступних машинних носіях:

- жорсткі диски (HDD, вінчестери) з інтерфейсами – PATA (IDE), SATA, у формфакторі – 3.5”, 2.5”, 1.8”, 1.0”;
- Raid-масиви;

- зовнішні накопичувачі HDD з інтерфейсом USB, Esata, Fibre Channel;
- USB накопичувачі (флешки), MP3- і медіа плеєри;
- карти пам'яті: CF (Compactflash), SD (Secure Digital), mini SD, microSD, Memorystick Pro/Pro Duo, MMC (Multimedia Card), RS-MMC, xd-Picture;
- SSD накопичувачі (Solid State Drive);
- CD- / DVD- / Floppy- диски.

Кращі фізико-технічні та математичні методи відновлення інформації за даними сервісного центру ТОВ «ЕПОС» дозволяють відновити понад 90% інформації.

Рис. 11.2 Руйнування дисководу (HDD)

Вихід з ладу магнітних голівок, заклинювання двигуна, зсув пластин і т.п. – одні із самих складних випадків втрати інформації (Рис. 11.2).

Для відновлення даних найчастіше необхідно розбирати не тільки несправний вінчестер, але й аналогічні робочі для з'ясування деталей функціонування. Роботи з розкриття жорстких дисків можна виконувати тільки в спеціальному приміщенні - герметичній камері з мінімізованим вмістом у повітрі пилу. Спроби розкриття корпусу HDD зовні такого приміщення можуть призвести до незворотної втрати інформації.

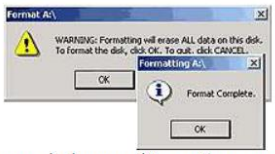


Рис.11.3 Знищення інформації засобами операційної системи

Основне правило після випадкового видалення даних – якнайменше звертань до жорсткого диска. Чим менше разів включався комп'ютер і чим менше даних було записано на вінчестер після видалення, тим вище ймовірність та повнота відновлення інформації при руйнуваннях логічної структури.

Руйнування логічної структури, переформатування призводять до втрати доступу до розділів диска, зникненню елементів файлової системи, відображенню розділів як неформатованих. Як і в попередньому випадку, важливо мінімізувати кількість звернень до диску. Тому робота ведеться тільки з точною посекторною копією диска, без внесення змін у логічну структуру накопичувача, що дозволяє уникнути помилок при відновленні інформації.

При руйнуванні службової інформації жорсткий диск не визначається в BIOS або визначається некоректно. Для відновлення даних використовується спеціальне устаткування й програмне забезпечення, що дозволяють виправити помилки в службовій області накопичувача.

Виникнення дефектних секторів («bad»-блоків) часто спричиняє лавиноподібний процес руйнування поверхонь дисків. Щоб знизити ризик необоротної втрати даних, використовуються спеціальні технології, що дозволяють швидко й з мінімальними втратами зберегти інформацію.

Відмова електроніки жорсткого диска – одна з найбільш частих причин втрати даних. На противагу поширеній думці заміна контролера сучасного вінчестера автоматично не вирішує проблеми. Це пояснюється тим, що службова інформація про конфігурацію конкретного приводу, що включає дані про кількість голівок, розмітці диска й т.п., зберігається в мікросхемі BIOS на платі контролера. Для відновлення даних необхідно перепрограмувати BIOS вінчестера так, щоб привести у відповідність службову інформацію контролера й гермоблоку.

Іноді в результаті збою вінчестер мимовільно встановлює пароль на доступ до даних. Щоб відновити інформацію, необхідне зняття пароля, для чого використовується спеціальні програмні й апаратні засоби.

Технологічний процес відновлення доступу до інформації завжди починається з діагностики технічного стану накопичувача, що включає в себе: діагностику робочих поверхонь, тестування контролера, виконання тестів читання даних. Після визначення причини втрати доступу до даних вибирається відповідний спосіб його відновлення.

Якщо за результатами діагностики технічний стан жорсткого диска відповідає нормам (накопичувач справний), а втрата інформації відбулася внаслідок програмного збою (вплив вірусів, некваліфіковані дії користувачів, збої операційної системи), то для відновлення доступу до інформації використовується спеціалізоване програмне забезпечення, що дозволяє одержати доступ до даних на диску на рівні команд інтерфейсу. У цьому випадку говорять про відновлення доступу до даних на логічному рівні.

При наявності достатнього досвіду в багатьох випадках відновити доступ до інформації на справному жорсткому диску можна й без застосування спеціальних утиліт, користуючись тільки Diskedit. Справедливості заради необхідно помітити, що досвід необхідний і при застосуванні спеціальних утиліт. В автоматичному режимі навіть широко відома утиліта "Tiramisu" не в змозі правильно відновити послідовність кластерів, що містять той або інший файл. Проте, у випадку повної справності жорсткого диска доступ до даних можна відновити й самостійно. Важливо тільки розуміти, що з першої спроби вгадати правильну послідовність кластерів не вдається. Тому, щоб не втратити інформацію остаточно, усі роботи по відбудові інформації можна проводити тільки з копією жорсткого диска.

Саме тому наступним кроком після діагностики накопичувача є створення точної копії (образа) жорсткого диска. Створення копії жорсткого диска необхідно не тільки з метою убезпечити свою роботу. Поверхня диска може мати окремі ушкодження.

Ці ушкодження небезпечні тим, що супроводжуються появою усередині герметичної камери жорсткого диска дрібних твердих часток. Ці частки приводять до нових ушкоджень поверхні, причому цей процес носить

лавиноподібний характер. У результаті після декількох годин роботи накопичувача на значній площі поверхні дисків робочий шар стирається повністю.

Технологія відновлення доступу до інформації з несправного жорсткого диска суттєво відрізняється від відновлення даних на логічному рівні. У багатьох випадках відновити працездатність накопичувача вдається лише на нетривалий час. Наприклад, у результаті "ляпання" голівки ушкоджується як сама голівка, так і поверхня диска. Найчастіше саме це і є причиною розглянутої вище несправності. Вибиті з поверхні диска осколки, перебуваючи усередині герметичної камери, продовжують руйнувати робочий шар, що дуже швидко призводить до повної відмови накопичувача.

Якщо при перших ознаках несправності жорсткий диск приносять у сервісний центр, то, як правило, вдається врятувати більшу частину інформації. Більше того, вдається відновити деяку частину інформації навіть із ушкоджених ділянок пластин жорсткого диска. Для цього при створенні копії жорсткого диска використовується технологія адаптивного копіювання.

Суть її полягає у швидкому копіюванні інформації з непошкоджених ділянок і наступному багаторазовому (до 100 разів) зчитуванні інформації з пошкоджених ділянок. Потім проводиться статистична обробка результатів зчитування збійних секторів за допомогою методу максимуму правдоподібності. Критерієм успішного відновлення інформації є досягнення заданого граничного значення коефіцієнта вірогідності. У деяких випадках після процедури адаптивного копіювання потрібне проведення робіт по відбудові даних на логічному рівні.

Пошкодження поверхні пластин жорсткого диска є, напевно, найпоширенішою й небезпечною несправністю, але далеко не єдиною. Жорсткі диски можуть виходити з ладу по безлічі причин. Це й порушення теплового режиму, і підвищена вологість, і виробничі дефекти, і "ляпанці" голівки через зовнішні ударні впливи, і зношування внаслідок інтенсивної роботи.

У таблиці 1 наведені деякі типові несправності жорстких дисків і способи відновлення доступу до інформації.

Таблиця 1.

Типові несправності жорстких дисків і способи відновлення доступу до інформації

	Несправності	Особливості відновлення
1.	Часткове ушкодження голівок (без обриву)	Заміна блоку голівок на аналогічний. Потрібне розкриття камери
2.	Обрив голівок	Заміна блоку голівок на аналогічний. Потрібне розкриття камери
3.	Вихід з ладу ІіМС підсилювача комутатора.	Заміна ІМС підсилювача комутатора. Заміна блоку голівок на аналогічний. Потрібне розкриття камери
4.	Ушкодження робочих поверхонь	Адаптивне копіювання інформації. Потрібне розкриття камери
5.	Вихід з ладу ІМС керування шпиндельним двигуном	Заміна ІМС керування шпиндельним двигуном. Без розкриття камери
6.	Вихід з ладу ІМС підтримки зовнішнього інтерфейсу	Заміна ІМС підтримки зовнішнього інтерфейсу. Без розкриття камери
7.	Вихід з ладу ПЗП контролера	Заміна ПЗП контролера із записом коду точного аналога. Без розкриття камери
8.	Повний вихід з ладу контролера накопичувача	Заміна контролера цілком на точний аналог. Без розкриття камери

Таким чином, усі випадки відновлення доступу до інформації на жорстких дисках, що відмовили, можна розділити на дві великі групи: потребуючі розкриття герметичної камери й не потребуючі її розкриття.

У випадку, коли розкриття герметичної камери не потрібно, проблема відновлення інформації вирішується заміною контролера або чипа керування двигуном на аналогічний. У принципі, таку операцію кваліфікований користувач може виконати самостійно. Необхідно знайти повний аналог несправного жорсткого диска й акуратно переставити з нього контролер.

Відновлення інформації з ушкодженнями в камері (обрив або ушкодження голівок, відмова комутатора, дефекти й зношування робочої поверхні) вимагає розкриття гермоблоку, що, у свою чергу, вимагає застосування спеціального устаткування й, у першу чергу, наявність " чистої кімнати" - приміщення, у якому суворо контролюється концентрація зважених у повітрі дрібних порошин.

У неробочому стані голівки притискаються до пластин у спеціальній зоні, називаною зоною паркування. Вихід голівок у зону паркування виконується автоматично при зниженні швидкості обертання двигуна нижче номінальної або провалі напруги живлення. Оскільки поверхні дисків і голівки виготовляються дуже гладкими, те іноді спостерігається ефект "прилипання" голівки до диска. У цьому випадку, при подачі напруги на накопичувач голівки не встигають відірватися від поверхні починаючих обертання дисків і відбувається їхній перекіс або обрив. Ушкодження голівок можуть виникати й у результаті "ляпання" голівки, викликаного зовнішнім ударним впливом на робочий жорсткий диск. В обох випадках голівка починає дряпати поверхню диска, ушкоджуючи його поверхню.

Щоб відновити інформацію з такого накопичувача, необхідно замінити ушкоджену голівку або блок голівок повністю. У більш старих моделях жорстких дисків кожна голівка в блоці при виробництві юстирувалися під свою робочу поверхню, тому навіть в одному блоці голівки могли бути позиціоновані по-різному.

При заміні блоку голівок було необхідно калібрувати всі чотири голівки, що забирало багато часу, при цьому при спробах відновити дані ще більше ушкоджувалася поверхня диска. Щоб розв'язати цю проблему, було розроблено прецизійне обладнання для заміни і юстировки окремих голівок. Це обладнання дозволяє вилучити ушкоджену голівку, запресувати на її місце робочу й відкалібрувати її з точністю до одиниць мікронів.

У сучасних жорстких дисках з високою щільністю запису такої точності юстировки голівки вже недостатньо, оскільки ширина доріжок запису становить порядку десятих часток мікрон. Крім того, завдяки досягненням у технологіях виробництва жорстких дисків блоки голівок у накопичувачах однієї серії практично ідентичні. Тому при ушкодженнях окремих голівок повністю заміняється весь блок.

Розповсюдженою причиною відмов жорстких дисків є вихід з ладу попереднього підсилювача-комутатора в результаті кидків напруги або неправильного підключення напруги живлення. У старих моделях

накопичувачів мікросхема комутатора перебувала усередині камери. Це дозволяло виконувати її заміну без зняття блоку голівок.

Щоб забезпечити мінімальне загасання сигналу зчитування, у сучасних жорстких дисках підсилювач-комутатор розміщають безпосередньо на блоці голівок. У цьому випадку перед заміною мікросхеми необхідно зняти весь блок голівок, щоб уникнути перегріву дисків при ремонті та втрати інформації. Деякі виробники використовують безкорпусні мікросхеми комутаторів, які не підлягають заміні - у цьому випадку заміняють увесь блок голівок.

Заміна будь-якого елемента жорсткого диска негативно позначається на його характеристиках. Через неможливість точно відкалібрувати блок голівок збільшується кількість помилок читання. Після заміни підсилювача-комутатора звичайно знижується відношення сигнал/шум, що теж приводить до росту помилок. Тому при копіюванні даних з відремонтованого жорсткого диска на технологічний доцільно застосовувати алгоритм адаптивного копіювання. Але навіть при застосуванні алгоритму адаптивного копіювання голівка часто "зациклюється" на деяких доріжках, багаторазово намагаючись зчитати той самий сектор. Це приводить до того, що на зчитування інформації з такого жорсткого диска йде дуже багато часу - у середньому добу, а іноді й до місяця безперервної роботи. Якщо виконувати таке копіювання у звичайному приміщенні, голівка досить швидко зітре робочий шар до основи.

Герметизація камер деяких жорстких дисків забезпечується за допомогою спеціальної липкої стрічки, що наклеюється по периметру корпуса накопичувача. При ушкодженні цієї стрічки (при необережному обігу при транспортуванні або установці у вузькі кишені деяких корпусів комп'ютера) можлива ненавмисна розгерметизація камери.

Порушення герметизації може приводити до влучення усередину камери пилу, що руйнує голівки й робочі поверхні дисків. Такий накопичувач може ще працювати якийсь час, однак звичайно дуже скоро починається лавиноподібний процес виникнення збійних секторів і він виходить із ладу. Проте, якщо вчасно звернутися в центр відновлення інформації, інформацію ще можна буде врятувати. Жорсткий диск розкриють у чистій кімнаті, акуратно вичистять пил, що потрапив усередину камери. Потім дані будуть переписані на технологічний жорсткий диск.

Слід зазначити, що будь-яке розкриття камери жорсткого диска, навіть без заміни його вузлів, приводить до погіршення його роботи й у наслідку до виходу його з ладу. Середній термін служби накопичувача, камера якого розкривалася, не перевищує двох-трьох місяців. Потім починається швидкий ріст кількості збійних секторів, збільшується ймовірність помилок читання й жорсткий диск виходить із ладу остаточно. Саме тому розкриття камери жорсткого диска й ремонт елементів, розташованих у камері, проводиться тільки з метою відновлення інформації, а не з метою відновлення його працездатності.

Останнім часом почастішали випадки, коли користувачі намагаються самостійно відновити інформацію або відремонтувати жорсткий диск, розкриваючи при цьому його камеру. Це завжди приводить до остаточного

порушення його працездатності й дуже утрудняє відновлення даних. Наприклад, відбитки пальців із дзеркальної поверхні пластини вилучити вже практично неможливо. І якщо інформацію на початку диска, де звичайно зберігається операційна система, ще можна буде відновити, то користувацькі дані в середині й кінці диска можуть бути загублені безповоротно.

Подавати напругу живлення на накопичувач із відкритою камерою поза чистою кімнатою неприпустимо. Повітряний потік захоплює частки пилу, які починають руйнувати робочий шар. Залежно від швидкості обертання дисків частки пилу знищать робочий шар за один-дві години, стираючи його до основи, з якої виготовлені диски. Інформацію в цьому випадку відновити неможливо.

Описані вище методи дозволяють у більшості випадків відновити інформацію. Однак, можливості всіх цих методів обмежуються точністю механічного позиціонування голівок читання. У цей час розроблені й могутніші способи відновлення інформації, що засновані на візуалізації магнітних полів розсіювання. Ці способи дозволяють створювати візуальний образ робочих поверхонь носія з високим дозволом, достатнім для побітового дослідження інформації. Відомо більш десятка таких методів, але при високої щільності запису даних сучасних жорстких дисків найбільшими можливостями по відновленню інформації має метод зняття магнітної сигналограми, заснований на магнітній силовій мікроскопії. Найбільші труднощі при застосуванні магнітної силової мікроскопії викликає необхідність сполучення безлічі зображень різних ділянок поверхні диска.

За допомогою подібних систем можливе відновлення інформації в ряді випадків навіть після того, як на місце зберігання відновлюваного файлу багаторазово записана нові дані.

Трохи менш потужним, але зате значно більш дешевим є метод Біттера (метод "магнітних чорнил"). Здатність аналізу при візуалізації магнітних полів за методом Біттера обмежується розмірами часток феромагнітних часток у суспензії, використовуваної в процесі візуалізації. Проте, застосовувана в центрі відновлення інформації компанії ЕПОС суспензія дозволяє здійснювати візуалізацію магнітних полів для жорстких дисків обсягом до 4ГБ. Більше того, для дисків більшої ємності можна одержати зображення з деталізацією, достатньої для аналізу загальної структури диска й стану його робочої поверхні.

У порівнянні з іншими типами носіїв інформації Flash має ряд особливостей, серед яких можна виділити найбільш істотні:

- обмежена кількість циклів запису;
- наявність спеціальної резервної області;
- блокова організація пам'яті.

Такі особливості Flash пам'яті типу NAND приводять до необхідності використання виробниками накопичувачів спеціальних алгоритмів оптимізації використання чарунок Flash пам'яті при записі даних. Це приводить до того, що інформація в Flash пам'яті записується в кодованому виді. Відсутність інформації про принципи кодування (що є комерційною таємницею багатьох

виробників Flash накопичувачів), і велика кількість кодів ускладнює процес відновлення інформації.

Специфіка фізичних і математичних принципів запису інформації у накопичувачів типу Flash пам'яті потребує застосування адекватних технологій.

Наприклад, розроблений ТОВ «ЕПОС» комплекс EPOS Flashextractor – є за суттю професійним рішенням для відновлення даних с флеш накопичувачів, що базується на технології фізичного доступу до Flash пам'яті. Комплекс являє собою друге покоління систем відновлення інформації з Flash. Основними відмінностями нової версії стали підвищена (в 2-3 рази) швидкість читання мікросхем пам'яті, вбудовані засоби корекції помилок зчитування й керування напругою живлення чипів.

Основні функції комплексу:

- Відновлення даних з будь-яких типів накопичувачів на основі Flash, у тому числі фізично несправних;

- Відновлення даних з Flash накопичувачів, що захищені за допомогою паролю.

Комплекс EPOS Flashextractor підтримує наступні типи флеш накопичувачів:

- USB Flash диски;

- SSD накопичувачі;

- карти пам'яті Secure Digital (SD card), Compactflash, xd Card, Memory Stick, Multimedia Card (MMC), Smartmedia і ін.;

- Flash - пам'ять цифрових фотоапаратів, диктофонів, мобільних телефонів, MP3 - плеєрів, кишенькових комп'ютерів.

Комплекс дозволяє подолати багато труднощів, що обумовлені швидкими змінами у принципах побудови та протоколах функціонування сучасних накопичувачів типу Flash пам'ять. Він забезпечує зчитування даних з максимальною швидкістю, яка обмежена тільки швидкодією мікросхем пам'яті. Для сучасних 16-розрядних чипів вона досягає 3,5 ГБ/хв. Вбудована технологія корекції помилок гарантує максимальну вірогідність зчитуваних даних. У комплексі реалізована підтримка найсучасніших протоколів читання з мікросхем пам'яті. Це дозволяє коректно витягати дані з мікросхем усіх типів і ємностей будь-яких виробників. Забезпечена підтримка трьох різних рівнів напруг живлення, а також можливість роботи із чипами пам'яті, що мають дві напруги живлення.

Знищення інформації в комп’ютерних системах

Нерідко старі комп'ютери (разом з жорсткими дисками) вивозяться разом з усіма даними, на захист яких були витрачені гроші й час; у великих організаціях це відбувається майже щодня.

У той час, як існують не тільки закони, але й апаратні засоби, що забороняють або перешкоджаючі несанкціонованому доступу до конфіденційної інформації, зняття даних зі списаного НЖМД дозволяє зацікавленій особі не тільки обійти системи безпеки без прояву зовнішніх ознак, але й зробити це практично законно.

Багато керівників організацій і користувачів комп'ютерів не знають, що просте видалення файлів або навіть переформатування жорсткого диска фактично не видаляє дані. Варто тільки якось записати інформацію на НЖМД і вилучити її з магнітної пам'яті диска буде дуже складно. Тому, видалося б, нешкідливий акт списання старого комп'ютера або передача його в іншу організацію - найбільш простий шлях відкриття доступу до інформації з обмеженим доступом.

Крім тієї конфіденційної інформації, про яку знають користувачі (бухгалтерської, фінансової, особистої, перспективні розробки), на ПК може зберігатися безліч інших конфіденційних даних, які не завжди відомі операторові. Додатки й операційні системи зберігають паролі, ключі шифрування й інші дані з обмеженим доступом у різних місцях, включаючи файли конфігурації й тимчасові файли. Операційні системи довільним образом записують уміст пам'яті у файл підкачування на диску, що не дає можливості довідатися, що із цих даних дійсно збережене на носії.

Забезпечення надійного знищення корпоративної інформації наприкінці життєвого циклу НЖМД вимагає ретельного опрацювання питань безпеки інформації.

Видалення даних із НЖМД саме по собі не забезпечує захисту інформації. Процес захисту повинен ґрунтуватися на ряді погоджених методик, що забезпечують в остаточному підсумку високу ймовірність знищення інформації.

Хоча жодна з методик не може гарантувати 100% надійність знищення інформації, існують основні положення й умови захисту інформації:

1. Необхідність фізичного захисту НЖМД. Крадіжка ПК або окремих накопичувачів приводить до витоку інформації, тому необхідно забезпечити їхню фізичну схоронність із моменту закінчення строку експлуатації до одержання документованого підтвердження про знищення даних.

2. Систематичний контроль і ведення звітності. Систематичний контроль має на увазі відстеження накопичувачів, що вибувають із експлуатації, контроль процесу знищення інформації й складання звіту про відхилення в цьому процесі й допущених помилках. Необхідно фіксувати наступні відомості:

- унікальний ідентифікаційний код знищуваного накопичувача;
- дату й час знищення;
- ініціали виконавця;
- використану методику знищення.

Таким чином, процедура забезпечення захисту інформації, збереженої на НЖМД, повинна включати наступні дії:

1. Фізичний захист інформації, що включає в себе інвентаризацію й обмеження доступу до НЖМД.

2. Систематичний контроль над процесом заміни, передачі й знищення інформації на НЖМД.

3. Використання стандартизованих додатків і методик по знищенню інформації на НЖМД.

4. Систематична перевірка процесів знищення інформації на НЖМД.

5. Періодичний контроль надійності знищення інформації з довільно обраних НЖМД.

6. Вибір методик і способів для знищення інформації на несправних НЖМД, шляхом аналізу категорійності збереженої на них інформації.

7. Забезпечення процедури збору й знищення НЖМД.

8. Ведення звітності по кожному знищеному НЖМД.

У цей час існує кілька способів знищення інформації, що збережена на НЖМД. Знищення передбачає стирання або видалення інформації з жорсткого диска таким чином, що її неможливо відновити ні обробкою на комп'ютерах за допомогою спеціального ПО, ні за допомогою лабораторних засобів (наприклад, аналіз поверхні магнітних пластин за допомогою скануючого мікроскопу).

Способи знищення інформації на НЖМД діляться на три великих групи:

1. Програмні, в основу яких покладено знищення інформації, що записана на магнітному носії, за допомогою штатних засобів запису інформації на магнітних носіях. У випадку знищення інформації на НЖМД програмним методом, він може бути повторно використаний в інших ПК, після інсталяції нової ОС і додатків. Знищення проводиться найбільш простим і природнім способом - перезаписом інформації. Перезапис - це процес запису несекретних даних в область пам'яті, де раніше втримувалися секретні дані. Слід зазначити дуже важливу деталь - при перезаписі інформації працездатність НЖМД повністю зберігається, у випадку, якщо він був повністю справним. На зношеному або несправному НЖМД провести надійне знищення інформації практично неможливо.

2. Механічні, пов'язані з механічним ушкодженням основи, на яку нанесений магнітний шар - фізичний носій інформації.

3. Фізичні, пов'язані з фізичними принципами цифрового запису на магнітний носій, і засновані на перебудові структури магнітного матеріалу робочих поверхонь носія.

По способу впливу на накопичувач можливо виділити дві групи:

- без руйнування гермокамери й робочих поверхонь НЖМД;
- з руйнуванням НЖМД.

Програмні методи знищення інформації на НЖМД можуть реалізовувати:

1. Початковий рівень (рівень 0). Це найбільш проста й часто застосовувана форма знищення інформації на НЖМД. Замість повного очищення жорсткого диска в завантажувальний сектор, основну й резервну таблиці розділів записується послідовність нулів. Однак у цьому випадку дані на диску не знищуються, до них ускладнюється доступ. Повний доступ до інформації на НЖМД легко відновлюється за допомогою спеціальних програм аналізу секторів диска (Norton Diskedit, Winhex).

2. Рівень 1. Проводиться запис послідовності нулів або одиниць у сектори даних. При цьому знищується не тільки завантажувальна область, але й дані. Звичайним користувачам у цьому випадку практично неможливо відновити знищену інформацію. Проте, існує можливість відновлення інформації при стиранні перезаписом. В основі її лежать:

- помилки оператора й неправильне використання ПО;
- відмова ПО перезаписувати весь адресний простір диска;
- залишкова інформація в дефектних секторах;
- аналіз зон залишкової намагніченості й ефекті країв доріжок.

Відновити інформацію, вилучену цим методом, стандартними засобами неможливо. Для відновлення потрібні спеціальні знання і обладнання.

3. Рівень 1+. Використовуються декілька циклів перезапису інформації. Чим більше циклів перезапису інформації, тем складніше відновити вилучені дані. Це пов'язане з неточністю позиціонування голівки. Чим більше раз голівка перезапише дані, тем вище ймовірність, що вона зітре зони залишкової намагніченості на краях доріжки.

Алгоритми формування послідовностей, що прописуються в сектори даних, стандартизовані. Найбільш часто застосовані наведені в таблиці 2.

Таблиця 2.

Алгоритми знищення даних

Алгоритм	Зміст алгоритму
Посібник із захисту інформації МО США (NISPOM) Dod 5220.22-M, 1995 р.	Кількість циклів записи - 3. Цикл 1 - запис довільного коду. Цикл 2 - запис інвертованого коду. Цикл 3 - запис випадкових кодів. Примітка NISPOM забороняє використання цього алгоритму для знищення даних із грифом: "СОВ.СЕКРЕТНО" Альтернативні способи (відповідно до NISPOM): - розмагнічування; - фізичне руйнування
Стандарт VISR, 1999 р. (Німеччина)	Кількість циклів записи - 3. Цикл 1 - запис нулів. Цикл 2 - запис одиниць. Цикл 3 - запис коду із чергуванням нулів і одиниць.
ДЕРЖСТАНДАРТ Р50739-95г. (Росія)	Для класів захисту даних 1..3 Кількість циклів записи - 2. Цикл 1 - запис нулів. Цикл 2 - запис випадкових кодів. Для класів захисту даних 4..6. Один цикл запису нулів.
Алгоритм Брюса Шнейера (Bruce Schneier)	Кількість циклів записи - 7. Цикл 1- запис одиниць. Цикл 2 - запис нулів. Цикли 3..7 - запис випадкових кодів
Алгоритм Пітера Гутманна (Peter Gutman)	Кількість циклів - 35. Цикли 1..4 - запис довільного коду. Цикли 5..6 - запис кодів 55h, AAh. Цикли 7..9 - запис кодів 92h, 49h, 24h. Цикли 10..25 - послідовний запис кодів від 00, 11h, 22h і т.д. до Ffh. Цикли 26..28 - аналогічно циклам 7..9. Цикли 29..31 - запис коду 6Dh, B6h. Цикли 32..35 - аналогічно циклам 1..4.

Перезапис утрудняє процес відновлення інформації, але така можливість залишається. Для відновлення інформації потрібно дуже дороге й складне встаткування й ПО.

Перезапис інформації на НЖМД може проводитися як на ПК, так і поза ним за допомогою спеціальних приладів, наприклад, виріб EPOS Tester HDD (рис. 11.4).

Рис. 11.4 EPOS Тестер HDD із програмним методом знищення інформації

Висновки по програмних методах знищення інформації на НЖМД:

Недоліки:

- Низька надійність знищення інформації. Після застосування програмних методів стирання інформації перезаписом є можливість відновлення інформації кваліфікованим експертом за допомогою або без спеціальних засобів.

- Тривалий час перезапису інформації носія (десятки хвилин, годинник). При багаторазовому перезапису час знищення інформації для одного носія множиться на кількість проходів.

- Перезапис інформації можливий тільки на справному НЖМД.

Переваги:

- Є можливість повторного використання НЖМД;

- Низька ціна й вартість експлуатації ПО або спеціальних засобів.

Ухвалення рішення про вибір методу знищення інформації часто пов'язане з оцінкою ризиків.

Тому вибір методу знищення інформації шляхом перезапису тісно пов'язаний з відповідями на запитання:

- Яка ймовірність потенційної загрози?

- Які зусилля може прикласти зловмисник для відновлення обмеженої до доступу інформації?

- Якщо його дії увінчаються успіхом, які можливі наслідки?

Механічні (фізичні) методи знищення даних на НЖМД застосовують, за звичай, коли необхідна підвищена надійність знищення інформації, при цьому руйнується сам носій інформації.

Вартість накопичувачів на жорстких дисках значно знизилася за останні роки. Тому, як і у випадку гнучких магнітних дисків, для багатьох компаній може бути економічно доцільно знищувати їх, а не видаляти секретну інформацію. Але тут ми зустрічаємося із проблемою високої вартості обладнання для механічного знищення й процесом контролю знищення у випадку наявності цього обладнання.

Механічні методи знищення інформації підрозділяються на:

• Механічного впливу. Здрібнювання носія шляхом пропущення через обладнання здрібнювання (шредер). НЖМД руйнується механічно так, щоб виключити можливість прочитання інформації яким-небудь способом з його робочих дисків. При цьому методі існує небезпека, що при здрібнюванні можуть залишатися фрагменти, досить великі, щоб відновити інформацію в лабораторних умовах. Розкриття корпуса гермокамери в робочому приміщенні

(поза чистою кімнатою) приводить до забруднення пластин і висновку НЖМД із ладу. У сучасному НЖМД пил, як наждаком, стирає робочий шар до основи (прозорої скляної підложи) уже через кілька годин роботи з розкритою гермокамерою. Часто використовувані на практиці методи свердлення отворів і удари молотком по приводу насправді зовсім не знищують або знищують тільки малу частину інформації.

• Термічні. Нагрівання носія до температури плавлення в спеціальних печах. При цьому способі гарантія знищення інформації наступає при розігріві носія до температури 800-1000оС. У цьому випадку інформація стає абсолютно не відновлюваної по цілому комплексу причин, у тому числі й через перехід магнітного матеріалу робочого шару через точку Кюрі. Такий спосіб знищення інформації може бути рекомендований для носіїв, що містять державну таємницю. Зауважимо, що пожежа в приміщенні, де перебувають НЖМД не приводять до знищення інформації.

• Піротехнічні. Руйнування носія вибухом.

• Металотермічні. Знищення підложи диску, на яку нанесене магнітне покриття.

• Хімічні. Руйнування робочого шару або основи носія хімічно агресивними середовищами.

• Радіаційні. Руйнування носія іонізуючими випромінюваннями.

У таблиці 3 наведені основні показники механічних методів знищення інформації на НЖМД.

Таблиця 3.

Фізичні методи знищення інформації на НЖМД

Методи	Зміст	Результат
Механічні	Здрібнювання носія, його руйнування механічним впливом.	Руйнуючий метод. Можливо гарантоване знищення.
Термічний	Нагрівання носія до температури руйнування його основи	Руйнуючий метод. Гарантоване знищення.
Піротехнічний	Руйнування носія вибухом	Руйнуючий метод. Можливо гарантоване знищення. Проблема забезпечення безпеки оператора.
Металотермічний	Знищення основи носія шляхом високотемпературного синтезу	Руйнуючий метод. Гарантоване знищення.
Хімічний	Руйнування робочого шару або основи носія хімічно агресивними середовищами.	Руйнуючий метод. Гарантоване знищення. Проблема забезпечення безпеки оператора.
Радіаційний	Руйнування носія іонізуючими випромінюваннями	Руйнуючий метод. Небезпека опромінення.

Деякі з наведених методів екологічно небезпечні, інші можуть забезпечити високу надійність знищення інформації, але вимагають настільки специфічного й коштовного обладнання, яке можуть дозволити собі лише деякі корпоративні користувачі.

Всі ці методи виключають можливість подальшого використання НЖМД.

Фізичні способи пов'язані з фізичними принципами цифрового запису на магнітний носій, і засновані на перебудові структури магнітного матеріалу робочих поверхонь носія. Найбільше широко застосовується вплив на робочу поверхню жорсткого диска магнітним полям. У силу певних особливостей конструкції жорстких дисків і застосовуваного в них способу запису в цей час застосовується в основному вплив потужним магнітним імпульсом з метою намагнічування робочої поверхні до насичення.

Таким чином, залежно від того, від яких загроз необхідний захист, можна вибрати адекватний метод знищення інформації. При цьому вірогідність знищення інформації повинна бути підтверджена тем або іншим способом.

Особливо це відноситься до методів знищення інформації, при яких зовні диск залишається неушкодженим.

Найбільші труднощі викликає підтвердження надійності знищення інформації шляхом впливу магнітного імпульсу. Фактично в цьому випадку придатні тільки різні методи візуалізації магнітних полів розсіювання.

Для підтвердження знищення інформації не обов'язково її повністю відновлювати. Але якщо в процесі контролю якості знищення будуть виявлені залишки інформації, то при застосуванні більш складних методів її можна буде відновити.

Тому для завдань контролю якості знищення інформації найбільш придатний метод Біттера. Більше того, завдання контролю якості знищення інформації (принаймні, при знищенні інформації впливом магнітного імпульсу) можна ще більш спростити.

Дійсно, синхродоріжка на поверхні жорсткого диска записується при виготовленні диска набагато могутнішим полем, ніж під час експлуатації диска записуються дані. Тому, якщо на поверхні диска не виявлені залишки синхродоріжки, те можна гарантувати, що всі дані тим більше знищені. Наявність же синхродоріжки після візуалізації магнітних полів методом Біттера можуть бути виявлені навіть без застосування мікроскопа.

Розслідування комп'ютерних інцидентів

У зв'язку зі швидким розвитком інформаційних технологій і зростанням цінності інформації, що зберігається на електронних носіях, комп'ютери й комп'ютерні мережі все частіше стають об'єктами таких незаконних дій як:

- несанкціоноване вторгнення, хакерські й DoS атаки;
- модифікація, викривлення або знищення баз даних;
- розкрадання або копіювання конфіденційної інформації;
- блокування доступу до інформації й базам даним;
- розкрадання коштів, шахрайство із платіжними засобами (банк-клієнт і ін.);
- використання вірусів і іншого шкідливого програмного забезпечення;
- несанкціоноване використання ПК для організації масових атак і інших шкідливих дій на інші ПК і локальні мережі.

забезпечення інформаційної безпеки в організації з метою мінімізації зазначених ризиків з однієї сторони вимагає застосування спеціальних систем і заходів, спрямованих на запобігання таких несанкціонованих дій, а з іншого

сторони – розслідування що відбувся таких IT-інцидентів з метою виявлення каналів витоку інформації, «дір» у системі інформаційної безпеки, виявлення «інсайдерів» і інших порушників безпеки.

Прикладною наукою про розслідування інцидентів і злочинів, пов'язаних з комп'ютерною інформацією, є комп'ютерна криміналістика ("Computer Forensics") . Сам термін "Forensics" є скороченою формою від "Forensics science", тобто судова наука або наука про дослідження доказів, і відбувся від латинського "foren", що означає «мова перед форумом», тобто виступ перед судом. У українській мові поки не встоялося загальновживаного терміна, однак усе частіше вживається термін «форензіка», що означає саме комп'ютерну криміналістику.

При розслідуванні IT-інцидентів дуже часто виникає завдання відновлення інформації після таких впливів як: несанкціоноване втручання в роботу ПК і локальних мереж, впливу шкідливих програм, недбалості співробітників, аварій, нещасних випадків, у тому числі й при фізичнім руйнуванні носія. Тому багато відомих компаній по відновленню інформації почали у свій час надавати й послуги з розслідування IT - інцидентів (наприклад, американська Ontrack, англійська Vogon і інші) . Не стала виключенням і українська компанія ЕПОС, що почала надавати такі послуги після 15-літнього досвіду в сфері відновлення інформації.

Порядок розслідування IT – інцидентів (ТОВ ЕПОС) базується на відомій моделі, що включає в себе чотири основні етапи:

1. Оцінка ситуації
2. Збір даних
3. Аналіз даних
4. Звіт про розслідування

Етап збору даних є дуже важливим етапом розслідування, у якому доводиться використовувати різні технології, методи, системи й обладнання. На цьому етапі проводиться відновлення інформації з накопичувачів.

Якщо накопичувач несправний, то попередньо проводяться роботи по відбудові його працездатності з використанням спеціальних апаратних і програмних засобів. Враховуючи, що аналіз інформації з електронних носіїв повинен проводитися без внесення будь-яких змін у їхній уміст, те основним елементом при відновленні інформації й збору даних є не руйнуюче копіювання інформації з досліджуваного на проміжний носій. Незважаючи на гадану простоту, операція копіювання даних являє собою непросте технічне завдання й вимагає застосування спеціальних апаратних і програмних засобів, які при розслідуванні IT-інцідентів повинні:

- Забезпечити копіювання всієї інформації на носії, у тому числі й схованої інформації (даних у схованих зонах, вільних блоків, «хвостів» файлів…), тобто створення повного образа накопичувача;
- Не вносити які-небудь зміни у вміст досліджуваного накопичувача (оригіналу);
- Мати можливість порівняння (верифікації) копії й оригіналу;

- Забезпечити необхідну вірогідність копії й оригіналу й виявлення помилок;

- Забезпечити досить високу швидкість копіювання.

Інформація може бути скопійована за допомогою програмних продуктів, наприклад, таких як Encase, а також програм DD зі складу ОС Linux або Freebsd. Однак на практиці фахівці віддають перевагу апаратним засобам.

Одним з відомих портативних апаратних засобів що забезпечує неруйнуюче копіювання інформації з інтерфейсів IDE, SATA, SCSI, USB й створення повного образа жорсткого диска є Imagemasster Solo-3 Forensic.

Для того щоб упевнитися у відповідності копії й оригіналу, використовують режим верифікації. Для забезпечення високої вірогідності верифікації використовують хеш-функції, що перетворюють вихідну інформацію в ключове слово - дайджест повідомлення. Якщо значення ключового слова оригіналу збігається з обчисленим дайджестом копії, то вважається, що скопійована інформація повністю відповідає оригіналу.

Обладнання Imagemasster Solo-3 Forensic підтримує декілька стандартів хеш-функцій: MD-5, SHA-1, SHA-2, що дозволяє експертові вибрати найбільш прийнятний алгоритм.

Слід враховувати, що при фізичних руйнуваннях жорсткого диска (вихід з ладу блоку голівок, заклинювання двигуна, подряпини й інші пошкодження поверхонь) не тільки роботи з його відновлення, але найчастіше й операції копіювання повинні проводитися в «чистій» кімнаті з регламентованим змістом пилу в повітрі.

При копіюванні інформації з жорстких дисків, що мають різного роду дефекти й руйнування, особливе значення набуває швидкість копіювання інформації. Дійсно, копіювання образа диска ємністю 1Тб у режимі PIO-4 становить близько понад 100 годин, а такий час більшість дисків з дефектами просто не зможуть відпрацювати.

Тому для копіювання жорстких дисків з дефектами необхідно використовувати апаратні засоби, що мають високу швидкість копіювання й можливість адаптивного копіювання й статистичної обробки результатів читання, що дозволяє зчитувати тільки потрібну інформацію й забезпечити максимально можливий відсоток успішно ліченої інформації.

Сучасне обладнання копіювання даних використовує максимально можливу швидкість, обмежену тільки можливістю інтерфейсу накопичувача. Так обладнання «Дискмастер» виробництва компанії ЕПОС забезпечує максимально можливу швидкість обмежену лише можливістю інтерфейсу - 3,5Гб/с, що дозволяє практично в 10 раз підвищить швидкість копіювання в порівнянні зі стандартними засобами, що працюють у режимі PIO-4. Крім того, на відміну від стандартних засобів, «Дискмастер» має можливість адаптивного читання дефектних секторів.

При копіюванні інформації Usb-Накопичувачів (флеш-пам'яті, зовнішніх жорстких дисків) необхідно використовувати апаратні блокатори запису, оскільки під ОС Windows відсутня можливість підключення накопичувачів без можливості запису на нього, а під ОС UNIX або Linux хоча і є така можливість,

однак найчастіше потрібні відповідні драйвера, щоб накопичувач міг бути пізнаний.

Відновлення й копіювання даних із флеш-носіїв має свої особливості. Так при копіюванні із флеш-накопичувача відсутня можливість копіювання інформації з резервних зон, у яких можуть перебувати, що цікавлять експерта вилучені або зруйновані файли й навіть цілі каталоги.

Для забезпечення гарантованої можливості копіювання всієї інформації, що міститься на флеш-накопичувачі необхідно використовувати спеціальні флеш-рідери, робота яких заснована на методі прямого доступу до пам'яті. Крім того, дані на флеш-пам'яті записані до кодованому виді.

Для адаптивного читання флеш-пам'яті використовується "EPOS NAND flash reader" . В обладнанні реалізована можливість виправлення помилок при читанні дефектних комірок пам'яті, що дозволяє зчитувати інформацію із флешпам'яті з великою кількістю дефектних комірок, зчитати інформацію з яких було неможливе ні за допомогою стандартних, ні за допомогою сучасних спеціальних рідерів, призначених для використання при відновленні даних.

Особливу складність при відновленні інформації із флеш-накопичувачів визначає наявність вбудованих у службову пам'ять флеш-накопичувача алгоритмів кодування. Алгоритми кодування даних є комерційною таємницею виробників флеш-обладнання, оскільки від цього алгоритму залежать такі критично важливі параметри як їхня швидкість роботи й надійність.

Ці алгоритми постійно вдосконалюють, поліпшуючи ті або інші характеристики флеш-накопичувачів, у підсумку чого з'являється безліч різних версій алгоритмів навіть для однієї й тієї ж моделі накопичувача, що ускладнює можливість їх розкриття в прийнятний термін.

Особливо складні алгоритми використовуються в SD-накопичувачах. Для декодування цих алгоритмів необхідно використовувати спеціальні системи декодування, наприклад, "EPOS Irs-flash", яка дозволяє автоматизувати процес розкриття алгоритму кодування даних аналізованої флеш-пам'яті.

Процес збору й відновлення даних може бути утруднений і при використанні паролів. Розкриття пароля не завжди являє собою тривіальне завдання. Так, у ноутбуках деяких виробників є можливість включення пароля для інформації на жорсткому диску на рівні BIOS.

Такий пароль захищає інформацію від несанкціонованого доступу при втраті або крадіжці ноутбука.

Іноді й користувач навмисно або ненавмисно «забуває» пароль. Досить складно розкривати й деякі програмні паролі, наприклад, поставлені на файли RAR або Microsoft Office. Використання програмних засобів для розкриття пароля займає іноді вельми тривалий час навіть при використанні швидкісних комп'ютерів.

Для прискорення розкриття пароля необхідно використовувати апаратні засоби, наприклад такі як COBRA (Code Brake Accelerator) . Одне таке обладнання забезпечує швидкість добору паролю до 2000 паролів у секунду для файлів Microsoft Office і до 300-500 паролів у секунду для файлів RAR не залежно від продуктивності комп'ютера. Обладнання має гарну

масштабованість і дозволяє поєднувати до 4-х таких обладнань в один блок. При цьому швидкість добору паролів зростає практично пропорційно кількості використовуваних пристроїв у блоці. Більше того, можна використовувати кілька таких блоків, підключених через USB до одного комп'ютеру.

Після копіювання й відновлення інформації необхідно забезпечити надійне зберігання отриманих даних. Звичайно робиться кілька копій (мінімум дві) отриманої інформації або дані зберігаються на сервері з відмово стійкою RAID-системою.

З метою запобігання несанкціонованого доступу до інформації копії перебувають у звичайному або так званому «інформаційному» сейфі. Інформаційний сейф «Кольчуга» являє собою систему миттєвого знищення інформації на одному або декількох жорстких дисків в RAID-системі при спробі крадіжки або несанкціонованого фізичного доступу до сервера або ПК.

Команда на знищення інформації може бути подана автоматично або по команді з радіо-брелока або мобільного телефону. Обладнання має автономне джерело живлення й дозволяє робити знищення інформації навіть при відсутності напругі мережі електроживлення.

У такий спосіб розвиток технологій відновлення інформації, розроблення систем і обладнання дозволяє розширити сферу послуг в області розслідування комп'ютерних інцидентів.

ТЕМА 10. Особливості методів захисту різних видів інформації з обмеженим доступом

Сутність метрики в системах безпеки

Створення систем забезпечення безпеки інформації повинно виходити що найменш з двох взаємно суперечливих принципів: достатності обраних заходів та засобів захисту щодо протидії реальним загрозам та мінімізації витрат наявних матеріальних, фінансових та людських ресурсів для реалізації плану захисту.

В загальному випадку велика кількість різноманітних засобів захисту, що використовують різні методи захисту, дозволяє побудувати різні за складом елементів системи та комплекси захисту.

Виникає питання, яким чином характеризувати наближення сукупності характеристик вказаних систем до оптимального варіанту та відрізняти їх захисні якості? Таким чином мова їде про обрання певного вимірювального інструменту – своєрідної метрики для оцінки якості систем безпеки.

Нормативні документи системи технічного захисту інформації (НД ТЗІ) встановлюють таку метрику, що отримала назву критеріїв оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою:

- для визначення вимог з захисту інформації в комп'ютерних системах від НСД;
- для створення захищених комп'ютерних систем і засобів захисту від НСД;
- для оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки конкретної інформації, що вимагає захисту.

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від НСД, що реалізовані в комп'ютерних системах.
2. Орієнтири для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги двох видів:

- вимоги до функцій захисту - послуг безпеки;
- вимоги до гарантій.

В контексті зазначених критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n — унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів, а саме, раніше розглянутих конфіденційності, цілісності та доступності, а також спостереженості.

Події, що можуть призвести до витоку інформації з обмеженим доступом, становлять загрози конфіденційності. В разі необхідності обмеження можливості ознайомлення з інформацією, то відповідні послуги обираються згідно з розділом "Критерії конфіденційності" НД ТЗІ 2.5-004-99. В цьому розділі описані такі послуги: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Події, що можуть призвести до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку обмеження можливості модифікації інформації відповідні послуги треба шукати в розділі "Критерії цілісності" НД ТЗІ 2.5-004-99. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність і цілісність при обміні.

Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі "Критерії доступності". В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі "Критерії спостереженості". В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, згаданий документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

В НД ТЗІ 2.5-004-99 існує сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відображає поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру вказаних критеріїв наведено на рис. 12.1.

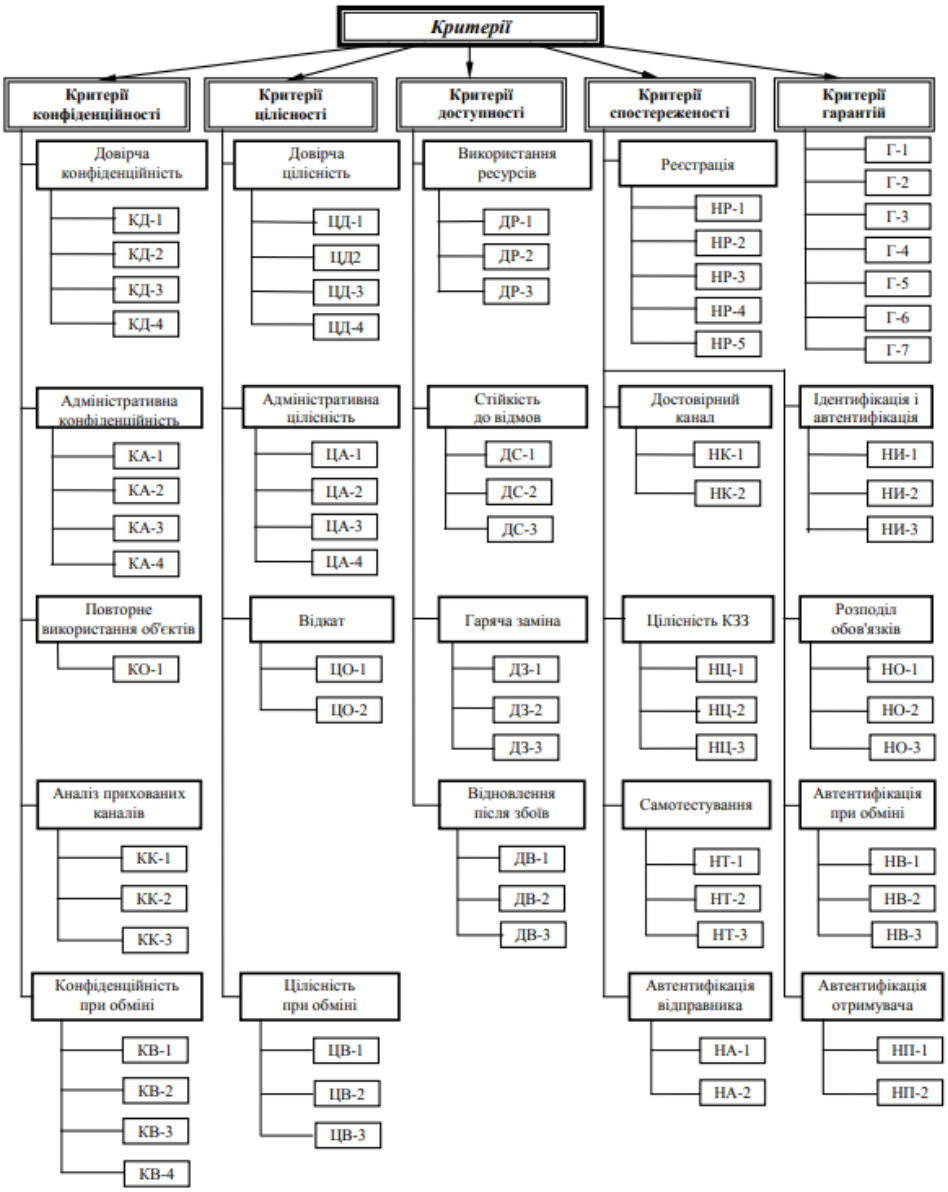


Рис.12.1. Структура критеріїв захисту згідно НД ТЗІ 2.5-004-99

В межах раніше визначених класів АС (АС1-АС3) на підставі вимог до забезпечення певних властивостей інформації - конфіденційності, цілісності і доступності виділяються такі підкласи АС, в яких підвищені вимоги:

- до забезпечення конфіденційності оброблюваної інформації (підкласи «х. К», до х – номер класу). Наприклад, підклас 1.К в разі АС класу 1.;
- до забезпечення цілісності оброблюваної інформації (підкласи «х.Ц»);
- до забезпечення доступності оброблюваної інформації (підкласи «х.Д»);
- до забезпечення конфіденційності і цілісності оброблюваної інформації (підкласи «х.КЦ»);
- до забезпечення конфіденційності і доступності оброблюваної інформації (підкласи «х.КД»);

- до забезпечення цілісності і доступності оброблюваної інформації (підкласи «х.ЦД»).
- до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»).

Для кожного з підкласів кожного класу в НД ТЗІ вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС.

Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Наведена класифікація корисна у плані спрощення процедури вибору переліку функцій, які повинен реалізовувати комплекс засобів захисту до проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Законом України «Про інформацію» визначено, що основними видами інформаційної діяльності є одержання, використання, поширення, захист та зберігання інформації. Одержання, використання, поширення, захист та зберігання документованої здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації.

Зокрема, Законом України "Про захист інформації в інформаційно-телекомунікаційних системах" (стаття 8) визначено, що інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Об’єкти захисту уточнені у «Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», що затверджені Постановою Кабінету Міністрів України № 373 від 29.03.2006. Захисту в системі, згідно пункту 4 згаданих Правил, підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування,

а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація).

Крім того, пункт 13 цих Правил встановлює, що передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв’язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Розглянемо більш детально специфічні вимоги щодо захисту конкретних видів інформації.

Основні заходи щодо захисту державної таємниці

Вихідні вимоги щодо захисту державної таємниці встановлені Законом України «Про державну таємницю», яким передбачено (стаття 18), що з метою охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

- особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

- режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний та криптографічний захисти секретної інформації.

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлені Постановами Кабінету Міністрів України.

Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності передбачає, що органи державної влади, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження

діяльності, пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Службою безпеки України можуть створюватися спеціальні експертні комісії, до складу яких включати фахівців органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони:

- відповідно до компетенції, державних завдань, програм, замовлень, договорів або контрактів беруть участь у діяльності, пов'язаній з державною таємницею;

- мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;

- додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, використання державних шифрів та криптографічних засобів тощо;

- мають режимно-секретний орган, якщо інше не передбачено законом.

Керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, що провадять діяльність, пов'язану з державною таємницею, мають бути обізнані з чинним законодавством про державну таємницю.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт , що здійснюються органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами відомостей, що становлять державну таємницю.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених законом.

Органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям, що провадять діяльність, пов'язану з державною таємницею, за результатами спеціальної експертизи надаються відповідні категорії режиму секретності, що зазначаються Службою безпеки

України у дозволах на провадження діяльності, пов'язаної з державною таємницею.

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації, яким надано зазначений у цій статті дозвіл, набувають права на доступ до конкретної секретної інформації згідно з рішенням органів державної влади, уповноважених державним експертом з питань таємниць приймати такі рішення. За погодженням з цими органами здійснюється передача секретної інформації або її матеріальних носіїв органам державної влади, органам місцевого самоврядування, підприємствам, установам і організаціям, які мають дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Порядок надання, переоформлення, зупинення дії або скасування дозволу на провадження діяльності, пов'язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, форма дозволу на провадження діяльності, пов'язаної з державною таємницею, та категорії режиму секретності встановлюються Кабінетом Міністрів України.

Особливості захисту службової інформації

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;
- визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
- здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Особливості захисту персональних даних

Інформація про особу - це сукупність документованих або публічно оголошених відомостей про особу.

Основними даними про особу (персональними даними) є: прізвище, ім’я, по батькові, адреса, номер телефону, національність, освіта, професія, сімейний та соціальний стан, релігійність, стан здоров'я, дата і місце народження і т.ін.

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.

Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом.

Кожна особа має право на ознайомлення з інформацією, зібраною про неї.

Персональні дані охороняються Законом. (Закон України «Про захист персональних даних»).

Суб’єктами відносин, пов’язаних з персональними даними, є:

- фізичні особи;

- юридичні особи; органи державної влади та органи місцевого самоврядування, організації, установи і підприємства усіх форм власності;

- уповноважений з питань захисту персональних даних;

- спеціально уповноважений центральний орган виконавчої влади з питань захисту персональних даних.

Суб’єктами відносин, пов’язаних з персональними даними, можуть бути інші держави та міжнародні організації.

Об’єктами захисту є персональні дані, які обробляються за допомогою систем автоматизованої обробки чи за допомогою систем щодо оброблення картотек персональних даних.

Персональні дані за режимом доступу є інформацією з обмеженим доступом.

Персональні дані фізичної особи, яка претендує чи займає вибірну посаду (в представницьких органах) або посаду державного службовця першої категорії не відносяться до інформації з обмеженим доступом.

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством (Закон Україні «Про захист інформації в ІТС»).

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту

інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи (Закон України «Про захист інформації в ІТС»).

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Вимоги до забезпечення захисту інформації в системі (Постанова № 373 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах)

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Оператори обробки персональних даних повинні обробляти інформацію відповідно до існуючого законодавства (захист персональних даних (інформація про фізичну особу). При обробці персональних даних (ПД) також повинні враховуватися конституційні права та свободи людини у тому числі право на недоторканість приватного життя, особисте та сімейне життя.

Реалізація профілів захищеності може бути забезпечена системами захисту інформації, які зображені на рис. 12.1.

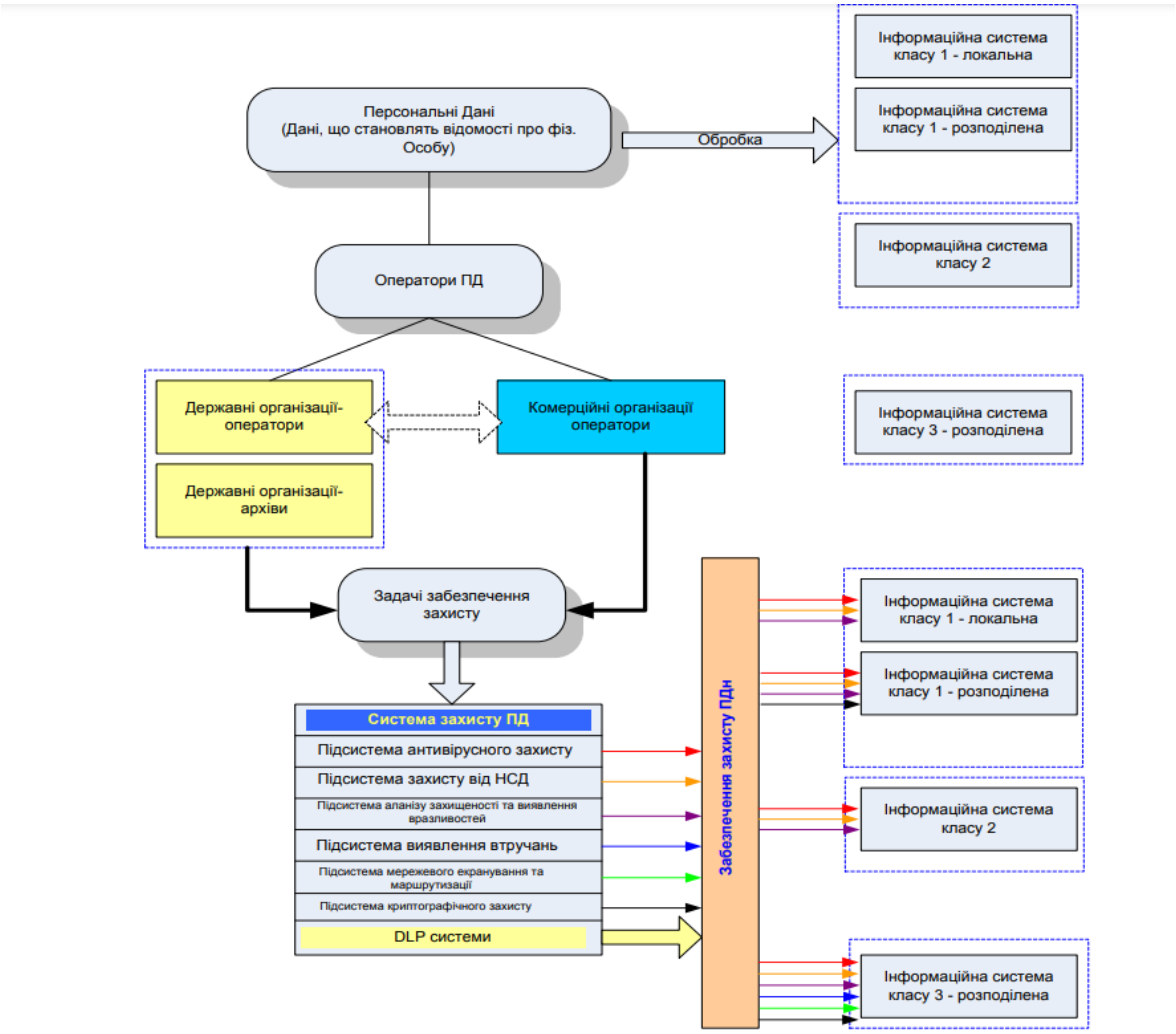


Рис. 9.1. Варіант побудови системи захисту персональних даних

Оператори обробки персональних даних повинні обробляти інформацію відповідно до існуючого законодавства (захист персональних даних (інформація про фізичну особу). При обробці ПД також повинні враховуватися конституційні права та свободи людини у тому числі право на недоторканість приватного життя, особисте та сімейне життя.

Доцільно реалізувати наступні етапи захисту персональних даних:

1) Визначити всі ситуації, коли необхідно виконувати їх збір, зберігання, передачу чи обробку.

2) Виділити процеси (або бізнес процеси), пов'язані з такими ситуаціями. Доцільно вибрати обмежене число процесів і проаналізувати їх. У рамках такого обстеження формується перелік підрозділів та співробітників компанії, що приймають участь у обробці персональних даних у рамках функціональних обов'язків.

3) Віднести персональні дані до певної категорії та класифікувати інформаційну систему.

4) Вибір та обґрунтування по зниженню категорій персональних даних, що обробляються інформаційною системою. Після чого формується актуальна модель загроз для відповідного типу інформаційної системи.

5) Розробити технічне завдання на створення відповідної системи захисту.

6) Провести уточнення класів інформаційної системи та підготувати рекомендації щодо використання технічних засобів захисту персональних даних.

Сучасні методи забезпечення надійності персоналу, як складової інформаційної безпеки

Основним джерелом створення матеріальних продуктів та послуг, що надаються підприємством є його персонал. Персонал фактично є творцем додаткової вартості та прибутків підприємства. Від якості управлінської діяльності у сенсі роботи з персоналом залежать практично усі складові діяльності підприємства, його економічний стан та його інформаційна безпека.

При цьому інформаційну безпеку підприємства у розрізі кадрової безпеки слід розглядати у двох аспектах:

• навмисних або випадкових дій персоналу «виробничих» підрозділів, які можуть створювати загрози для підприємства;

• непрофесійних або несумлінних дій співробітників, які включені до системи безпеки підприємства, внаслідок чого у системі безпеки можуть виявлятися вразливості.

Психологічний стан на різних етапах розвитку підприємства

Таким чином, кадрова безпека повинна створити належні умови для своєчасного виявлення джерела внутрішніх загроз підприємству (зрадник, інсайдер, крадій) та попередження виникнень вразливостей у системі безпеки підприємства.

Типовими найбільш поширеними проблемами на підприємствах, що пов’язані з прорахунками у кадровій роботі, з низкою мотивацією ефективної праці персоналу, наведені у таблиці 1.

Таблиця 1

Типові кадрові проблеми на підприємствах

Первинні проблеми	Вторинні проблеми
- Низька ефективність впливу керівників на підлеглих, організаційні проблеми; - Протиріччя у стосунках роботодавець – робітник, проблеми “суспільного співробітництва” у діяльності підприємства; - Неналежний стан системи стимулювання ефективної праці, слабкий зв’язок результатів праці виконавців та заохочень; - Низка ефективність методів нормативного визначення праці; - Слабка перспектива кар’єрного росту, що знижує робочий тонус співробітників; - Відсутність умов для самореалізації потенціалу співробітників; - Застаріле або недостатнє оснащення робочих місць; - Нерозвиненість соціальної та культурної сфер підприємства; - Недостатня увага навчанню та стажуванню (у т.ч. кадрового резерву).	- Висока конфліктність; - Низький рівень виконавчої дисципліни, халатне ставлення до роботи; - Низький професійний рівень персоналу; - Збої у виробничому процесі, неякісне виконання функціональних обов’язків, систематичний брак у роботі; - Низький рівень міжособистих комунікацій, незадовільний морально психологічний клімат, проблеми зі створенням узгодженої команди; - Незадоволеність співробітників роботою, висока текучість кадрів; - Негативна оцінка діяльності керівництва з боку персоналу; - Небажання співробітників підвищувати власну кваліфікацію; - Невідповідність реальної поведінки виконавця очікуванням керівника; - Нераціональність мотивів поведінки виконавців; - Безініціативність співробітників; - Проблеми роботи з певними категоріями персоналу («кар’єристи», «честолюбці», «правдошукачі» та «правдоборці» тощо).

Деякі з перелічених проблем тісно пов'язані, деякі в певних умовах є причинами для інших, а в інших умовах є наслідками. Можливо звернути увагу що на виникнення вказаних проблем також впливають об'єктивний стан розвитку підприємства та суб'єктивні мотиви поведінки особистостей.

Для аналізу подібних проблем та вироблення адекватних кадрових заходів и мотиваційної політики необхідно в першу чергу визначити у якому стані зрілості перебуває підприємство: становлення, функціонування, розвиток або криза. Виходячи з системного підходу аналізу частини через призму цілого, почнемо з особливостей етапів життя підприємства у цілому, після чого розглянемо аспекти мотиваційного менеджменту на цих етапах.

Зазвичай розрізняють наступні стадії існування підприємства.

Становлення підприємства – це стадія формування організаційної структури та колективу співробітників. Суттєвою рисою становлення є динамічність структури діяльності і складу працівників. Стадії становлення підприємства у випадку її нормального перебігу притаманні наступні характеристики, що наведені у таблиці 2.

Таблиця 2

Характеристика стадії ***Становлення підприємства***

Характеристика колективу	Коментар до характеристики
1. Оптимізм, ентузіазм, «бойовий» дух	Ці характеристики відображають підвищений мотиваційний фон, притаманний тим, хто починає нову справу, виходячи з власних мотивів. Без такого «бойового» духа або все скінчується досить швидко, або на виході «чистий нуль».
2. Усвідомлення об'єктивної необхідності нової діяльності	За звичай, нова діяльність є реакцією на соціальний заказ/попит, якій не задовольняється повністю або частково. Ця передумова - об'єктивна необхідність, на відміну від суб'єктивної, для якої головною є потреба суб'єкта, що зацікавлений у створенні нової діяльності.
3. Взаємопідтримка, колективізм, здатність діяти у складних умовах	Часто нова діяльність пов'язана з проблемами та труднощами, тому необхідною умовою її подальшого існування є взаємопідтримка, колективізм. За відсутності вказаних якостей різко знижується ймовірність переходу на рівень сталого функціонування.
4. Нормативна та технологічна творчість	Становленню діяльності властиві відсутність узгоджених норм взаємодії, чіткого розподілу функцій, технологічності у роботі тощо. Тому для даної стадії характерно прийняття де факто ініціатив співробітників з послідуючим їх узгодженням та нормативним оформленням. Таким чином створюється нормативна база (правила, задачі, функції, норми тощо), що передумовою переходу у стале функціонування.
5. Романтика перспектив нового підприємства, оперативність у діях та розвиненість ситуаційного почуття, інтуїція в діях	На етапі становлення, більш всього співробітників надихає перспектива, деякий ідеальний образ, що підтримує високу енергетику на шляху досягнення цілі. Характерною рисою цього етапу є почуття змін в умовах. Цей час життя підприємства характеризується тим, що рішення, в основному, за відсутності досвіду обираються інтуїтивно. Співробітники переважно не мають досвіду створення нового, не мають чітких алгоритмів дій та способів реагування на зміни в обстановці.
6. Значущість відповідності узгодженим «усним» нормам, оптимальність, справедливість	На початку шляху до цілі не має часу для юридичного оформлення розподілу завдань, тому характерним є висока значущість усних домовленостей між співробітниками, узгоджених провідними менеджерами, що виключає загрозу роздроблення спільного завдання на окремі незв'язані частини. Міра справедливості розподілу задач на цьому етапі має ключове значення: кожен робить те, що вміє, любить, що більш відповідає його можливостям, що узгоджено та взаємозалежно від інших співробітників.

Цей етап у житті організації є найбільш придатним для створення бази системи безпеки підприємства, оскільки не потребує перебудови встановлених зв'язків та правил. Але ж цей період є досить складним, оскільки не вистачає кваліфікованих фахівців, на прийняття рішень діють суворі обмеження часу,

велика ймовірність реалізації зовнішніх загроз, оскільки система безпеки має багато вразливостей.

Функціонування підприємства - це така система його діяльності, коли є в основному стабільна організаційна структура та сформований колектив співробітників. Відмінністю етапу функціонування є готовність підприємства реалізовувати різні замовлення без докорінної перебудови технологій та суттєвих змін у структурі.

Колективу нормально функціонуючого підприємства притаманні в основному властивості, що наведені у таблиці 3.

Таблиця 3

Характеристика стадії ***Функціонування підприємства***

Характеристика колективу	Коментар до характеристики
1. Жорстка нормативна дисципліна	Функціонування характеризується наявністю чітких норм діяльності та системи контролю за їх виконанням. Головна ознака етапу - визначеність норм та адекватність дій співробітників цім нормам. Також створені механізми підтримання нормативної дисципліни.
2. Готовність персоналу до підвищення кваліфікації та закріплення навичок	Оскільки функціонуванню властиві стабільність та дотримання норм, то для співробітників значно більше потрібна не творча ініціатива, а суворе виконання норм. Для більш адекватної відповідності нормам співробітники додатково навчаються, а також самостійно вдосконалюють навички у межах своєї функції. Готовність співробітників навчання становиться одним з головних критеріїв оцінки і підбору персоналу підприємства.
3. Сталість вертикальних і горизонтальних відносин та організаційної структури у цілому	Функціонуванню властиві закріплені нормативно сталі вертикальні і горизонтальні відношення. Як правило, ці відношення признані, прийняти та виконуються співробітниками без критичної напруги.
4. Домінування задачного, рутинізованого типу роботи	На відміну від становлення у функціонуванні переважує задачний режим роботи, у якому відомо, що і як робити, а співробітники мають необхідні навички для виконання своїх функцій (якщо ні – додаткове навчання). На цьому етапі в основному менше впроваджуються нові ідеї, від співробітників потрібен не стільки творчій підхід, скільки, навпаки, пильність, ретельність, методичність.
5. Сбалансованість між функціональних і міжособистих стосунків	Межі функцій чітко прописані і взаємодія представників різних функцій нормована і ретельно прописана, міжособисті взаємодії збалансовані, конфлікти переважно усунені та можливі типи відношень узгоджені та прийняти усіма членами команди.
6. Чіткість, операційність, технічність та заданість виконання норм	Нормативна база на етапі функціонування має конкретний, технологічний характер. Кожна функція доступна і зрозуміла співробітникам, чітко визначено коло задач і цілей кожної функції. Все це дозволяє кожному робітнику самостійно і адекватно реалізовувати поставлені задачі. Це також полегшується контроль виконання.
7. Консерватизм нормативної бази, відтворюваність основних технологічних процедур у разі незначної модифікації	Нормативна база переважно характеризується незмінністю та має для співробітників характер директивного припису. Корекція норм на етапі функціонування доволі рідка процедура, яку застосовують у надзвичайних випадках. Особлива цінність етапу – неухильне виконання встановлених норм. Співробітники, в основному, відтворюють одні і теж процедури у рамках встановленого циклу. У разі нагальної необхідності модифікуються лише несуттєві аспекти затверджених процедур.
8. Стабільність норм взаємодії співробітників	Взаємодія співробітників, по-перше, нормативно визначена, по-друге, в них сформовані необхідні навички з ефективної взаємодії. При стабільному функціонуванні рідкі конфлікти і взаємні претензії між співробітниками.
9. Сталий розподіл функцій	Кожен співробітник виконує визначені для нього функції і чітко розуміє власний внесок у спільну справу.
10. Налагодженість, збалансованість стосунків підприємства із зовнішнім середовищем	На відміну від етапу становлення, коли взаємодія з зовнішнім середовищем мали випадковий, слабо організований характер, стосунки етапу функціонування стабільні. Підприємство органічно взаємодіє з зовнішнім економічним, правовим, соціально-культурним та іншими середовищами. Взаємодія з зовнішніми структурами має технологічно-оформлений характер, тобто існує повна визначеність, з якого приводу, з кім і как необхідно взаємодіяти.

Етап функціонування найбільш приємний для підтримки високого рівня надійності системи безпеки підприємства та проведення його часткової модернізації.

Чітка регламентація стосунків підрозділів та співробітників, визначеність порядку дій, мінімальний рівень конфліктних ситуацій створюють позитивний фон для завчасного виявлення джерел можливих загроз, уникнення вразливостей системи безпеки. Повна перебудова системи безпеки на цьому етапі може створити масу проблем виробничому процесу та сприймається керівництвом вкрай негативно. Рішення про істотні зміни у концепції безпеки приймається лише після надзвичайних подій (варіант - терористичні атаки).

Таблиця 4 – Характеристика стадії Розвиток підприємства

Характеристика передумов	Коментар до характеристики
1. Криза попередніх форм діяльності	Криза попередніх форм діяльності виникає за умов вичерпаності або крайньої неефективності існуючих внутрішньо організаційних форм діяльності внаслідок їх морального старіння. Ознаками кризи є: неприпустимо низький рівень ефективності діяльності, зріст заборгованості і дефіцит фінансів, неухильне зниження прибутку, скорочення клієнтської бази, поширення та загострення міжфункціональних та міжособистих конфліктів тощо.
2. Суттєва зміна зовнішніх умов створює проблеми існування та вимагає від підприємства змін	Зовнішні умови, як сукупність економічного, правового, політичного, соціального, екологічного та інших середовищ, можуть змінюватися повністю або частково залежного від дій сил, що взаємодіють під час конкурентної боротьби. Ці зміни не дозволяють підприємству тривалий час використовувати стали норми.
3. Накопичення потенціалу для розвитку, включаючи технологічний, організаційний, професійний	Співробітники відчувають дефіцит можливостей для розкриття власного потенціалу у старих умовах, створюється бачення застарілості колишніх технологічних та інших норм, виникає нагальна потреба їх вдосконалення. Стратегія та цілі підприємства звужені, не відповідають сучасності та не мають перспективи. Засоби, способи і технології діяльності підприємства не дозволяють працювати ефективніше, виявляється потенціал для їх вдосконалення
4. Недосконалість системи управління та її нездатність оперативно вирішувати управлінські задачі	Існуюча система управління не відповідає вимогам ані виконавців ані керівників. Зростання чисельності штату підприємства призводить до збоїв у системі управління, збільшення часу реагування на події, ускладнення процедур доведення управлінських рішень до виконавців, попередні методи управління не дають дієвого ефекту, ускладнення взаємодія та злагодженість управлінських ланок.
5. Об'єктивна потреба підприємства у створенні нових підрозділів	Неможливість підвищення виробничих показників, виникнення нових задач та нездатність до їх опрацювання у рамках існуючої структури є об'єктивними передумовами до перерозподілу функцій, утворення нових структурних підрозділів, що забезпечать досягнення нових цілей та усувають проблеми міжфункціональної взаємодії, що відновлюються.
6. Зміна цільових орієнтирів	Постійні зміни потреб ринку у більш якісної продукції, нових продуктах або послугах, вимагають від підприємства змін або уточнення цілей щоб залишитися на ринку та збільшити прибуток.
7. Негативний прогноз на майбутнє, зріст проблем у випадку подальшого відтворення попередніх методів і способів роботи	Потреба вдосконалення підприємства може бути обумовлена негативними прогнозами на майбутнє для підприємства внаслідок зростання загрози тиску з боку конкурентів, якщо існуючи форми та методи діяльності підприємства не забезпечать збереження власних позицій.
8. Зростання конкуренції та зниження конкуренто спроможності продукції, виявлення нових, більш ефективних форм діяльності	Поштовхом до проведення докорінних змін на підприємстві може бути виявлення керівництвом нових ефективних технологій у виробничої, інформаційної, маркетингової та інших сферах.
9.Криза підприємства	Криза підприємства обумовлюється тривалим поєднанням двох факторів: проблемами поточного функціонування та ігноруванням негативних тенденцій управлінською ланкою.

Розвиток підприємства – це етап його діяльності, що характеризується реалізацією внутрішньо організаційних реформ, проведення яких обумовлено кризою попередніх форм діяльності та неможливістю їх відтворення. Ознакою підприємства, що розвивається є активізація та прискорення процесів

вдосконалення структури діяльності та залучення ресурсів, необхідних для адаптації організаційної структури до нових умов господарювання.

Зазначений етап є найбільш складним у плані забезпечення безпеки підприємства внаслідок ускладнення та загострення усіх проблем, скорочення часу для прийняття рішень, проявами негативних тенденцій у середовищі персоналу, міжособистими конфліктами, проявами суттєвих вразливостей у організаційно-технічній системі забезпечення безпеки підприємства.

Різні етапи підприємництва створюють об'єктивні передумови для формування мотиваційної політики на підприємстві та управління персоналом у аспекті його безпеки.

Кадрова складова інформаційної безпеки

Належний рівень інформаційної безпеки у великій мері залежить від складу кадрів, їх інтелектуального потенціалу й професіоналізму. Незадоволеність персоналу матеріальним становищем або рівнем соціальних гарантій є передумовою виникнення колізій у інформаційній сфері. Тому постійна увага цьому питанню, роботі з кадрами є одним з головних чинників забезпечення інформаційної безпеки.

Методи убезпечення (охорони) інтелектуальної й кадрової складової інформаційної безпеки охоплюють два взаємозалежні й у той же час самостійні напрямки діяльності того або іншого суб'єкта господарювання:

- перше - орієнтоване на роботу з персоналом підприємства (органу, установи), на підвищення ефективності діяльності всіх категорій персоналу;
- друге - націлене на збереження й розвиток інтелектуального потенціалу, тобто на охорону сукупності прав на інтелектуальну власність (у тому числі на патенти й ліцензії), а також на використання накопичених знань і професійного досвіду працівників підприємства (організації).

Першою стадією процесу забезпечення цієї складової інформаційної безпеки є оцінка загроз негативних впливів і можливих збитків від таких впливів.

Основні негативні впливи на інформаційну безпеку це недостатня кваліфікація працівників тих або інших структурних підрозділів, їх небажання або нездатність приносити максимальну користь своїй фірмі, готовність за гроші продати відому їм таємницю. Це може бути обумовлене низькою мотивацією персоналу, неефективним керуванням персоналом, відсутністю коштів на оплату праці окремих категорій персоналу підприємства (організації) або нераціональною їхньою витратою.

Процес планування й керування персоналом, спрямований на охорону належного рівня ІБ, повинен охоплювати організацію добору, наймання, навчання й мотивації праці необхідних працівників, включаючи матеріальні й моральні стимули, забезпечення соціальними благами, заходу щодо підвищення престижності професії, посиленню в ній творчого початку.

Важливою ланкою встановлення нормального рівня ІБ є оцінка ефективності заходів, здійснюваних шляхом зіставлення загальної величини витрат на попереджувальні заходи й втрат для підприємства (організації).

При цьому, оптимальна система мотивації праці повинна враховувати стадію, на якій перебуває організація : становлення, функціонування, розвиток.

Зовнішніми обмеженнями для оптимальної системи мотивації праці є:

- правове середовище: система мотивації повинна враховувати існуюче трудове та інше законодавство;

- економічне середовище: система мотивації повинна враховувати ситуацію на ринку праці та загальні економічні умови у державі, регіоні, галузі.

Для розуміння потреб персоналу, правильного формування мотиваційної політики підприємства може бути корисною модель потреб і мотивацій співробітників, так звана піраміда А.Маслоу (рис. 13.1).

З наведеної схеми можливо зробити висновок, що в основі потреб людини – фізіологічні потреби (здоров'я, відпочинок, їжа, притулок, транспорт) потреби безпеки та захищеності (впевненість у майбутньому, самозахист).

Вторинними потребами людини є соціальні потреби (дружба, схвалення, любов, належність до соціальної групи, порозуміння), потреби у визнанні (повага, авторитет, реальна влада, незалежність, успіх, самовдосконалення), потреби у самореалізації (досягнення життєво важливих цілей, свобода творчості, реалізація потенціалу).

Рис. 13.1 Мотиваційна модель поведінки персоналу по А.Маслоу

А.Маслоу сформулював два важливих для управління правила:

- слід задовольняти фізіологічні потреби, до то як апелювати до психічних;

- одного разу задоволена потреба більш не є мотивуючою.

Саме підприємство, намагаючись забезпечити не тільки прибуток, а й невід'ємний фактор стабільності – інформаційну безпеку, повинно для досягнення власних цілей сприяти у задоволенні потреб співробітника. Для цього на підприємстві повинна бути створена система мотивації праці.

Сучасними науковими дослідження визнано, що основними принципами оптимальної системи мотивації праці є наступні:

- Кожен труд повинен мати адекватну винагороду.

- Рівна винагорода за рівну працю.

- Система мотивації повинна забезпечувати адекватну мотивацію працівника до праці.

- Система мотивації повинна забезпечувати адекватне самовизначення працівника до кола своїх професійних завдань.

- Система мотивації повинна заохочувати такій труд персоналу, якій особливо цінний для організації.

Система мотивації повинна бути спрямована на підтримку необхідної якості та безпеці робіт, підтримку норм організації та її вдосконалення.

Основні акценти мотивації:

- при індивідно-суб'єктної спрямованості працівника – стабільність матеріального стимулювання; перспективи підвищення зарплати й соціального статусу;

- при суб'єктній спрямованості працівника – гарантованість більшої стабільності; організаційна підтримка; огородження від проблемного режиму шляхом постановки конкретних завдань; схвалення позитивних результатів у присутності колективу; стимулювання повноцінного, відкритого спілкування й довіра;

- при особистісній спрямованості працівника – стимулювання творчої активності; делегування вирішення проблем; стимулювання ініціативи аналізу й удосконалювання діяльності; доручення нового незвіданого фронту роботи; проява довіри до професіоналізму; залучення в співучасники в нормотворчості; підтримка в повідомленні ефективних ідей і шляхів їх реалізації в колективі.

Методи підвищення ефективності дій персоналу щодо забезпечення ІБ

Одним з основних напрямків захисту інформації в інформаційних системах від ненавмисних загроз є скорочення числа помилок користувачів і обслуговуючого персоналу, а також мінімізація наслідків цих помилок. Для досягнення цих цілей необхідно забезпечити:

- наукова організація праці;
- виховання й навчання користувачів і персоналу;
- аналіз і вдосконалювання процесів взаємодії людину із системою.

Наукова організація праці передбачає:

- належне устаткування робочих місць;
- оптимальний режим праці й відпочинку;
- дружній інтерфейс (зв'язок, діалог) людини із системою тощо.

Робоче місце користувача або фахівця із числа обслуговуючого персоналу повинне бути обладнане відповідно до рекомендацій ергономіки.

Висвітлення робочого місця; температурно-вологісний режим; розташування табло, індикаторів, клавіш і тумблерів керування; розміри й колір елементів устаткування, приміщення; положення користувача (фахівця) щодо встаткування; використання захисних засобів – усе це повинне забезпечувати максимальну продуктивність людини протягом робочого дня. Одночасно зводиться до мінімум стомлюваність працівника й негативний вплив на його здоров'я несприятливих факторів виробничого процесу.

Одним із центральних питань забезпечення безпеки інформації від усіх класів загроз (у тому числі й від навмисних) є питання виховання й навчання обслуговуючого персоналу, а також користувачів корпоративних інформаційних систем.

В обслуговуючого персоналу й користувачів системи необхідно виховувати такі якості як патріотизм (на рівні держави й на рівні корпорації), відповідальність, акуратність тощо.

Важливим завданням керівництва є також добір і розміщення кадрів з обліком їх ділових і людських якостей.

Поряд з вихованням фахівців велике значення в справі забезпечення безпеки інформації має й навчання працівників.

Далекоглядний керівник не повинен жалувати коштів на навчання персоналу. Навчання може бути організоване на різних рівнях. Насамперед, керівництво повинне всіляко заохочувати прагнення працівників до самостійного навчання. Важливо навчати найбільш здатних, працьовитих працівників у навчальних закладах, можливо й за рахунок установи.

ТЕМА 11. Елементи управління системою захисту інформації

Міжнародні стандарти у галузі інформаційної безпеки

Сукупність засобів захисту інформації та персонал, що обслуговує їх, повинні діяти за певною схемою, що забезпечуватиме найбільш ефективне застосування. Тому на основі кращих підходів була сформульована концепція створення системи управління інформаційною безпекою, яка згодом була детально визначена міжнародними стандартами.

В загальному випадку управлінська діяльність має власну методологію. Методологія управління (інакше – менеджменту, від англ. – management – управління) включає певні закони, цілі, принципи, методи, функції і технології управління а також практику управлінської діяльності.

В якості основного завдання створення системи управління в певній галузі, на об’єкті в організації висувається формування професійної управлінської діяльності.

Розрізняють декілька основних підходів щодо побудови системи управління, а саме процесний, системний та ситуаційний підхід.

Процесний підхід. Діяльність з виконання окремих функцій є процесом, що вимагає певних витрат ресурсів і часу. Саме процесний підхід до менеджменту дозволяє з’ясувати взаємозв'язок і взаємозалежність функцій управління.

Процес менеджменту відображає рекомендовану послідовність виконання основних функцій управління, точніше, послідовність початку дій по виконанню функцій, так як здійснення багатоконтурною зворотного зв'язку приводить до одночасного здійснення функцій.

Оскільки, необхідною умовою забезпечення якості реалізації наступної функції (етапу) є якісне виконання попередньої, ми об’єктивно бачимо взаємозалежність функцій.

Сполучними процесами є процес комунікацій і процес прийняття рішень.

Наприклад, в організації може реалізовуватися безліч процесів. Згаданий в попередніх розділах професор Гарвардської школи бізнесу Майкл Портер пропонує класифікацію процесів, яка базується на їх ролі в створенні додаткових цінностей (кожен процес повинен вносити додатковий внесок по відношенню до попереднього процесу в цінність кінцевого продукту).

Відповідно до цього критерію всі процеси поділяють на три групи:

- основні, які пов'язані безпосередньо з виробництвом продукції;
- забезпечити процеси здійснюють підтримку основних процесів (постачання, управління персоналом та інші);
- управлінські процеси включають процеси щодо встановлення цілей і формуванню умов для їх досягнення.

Всі перераховані процеси взаємопов'язані між собою і утворюють єдину систему.

Системний підхід. Дослідження управління як процесу призвело до широкого поширення системних методів аналізу. Застосування системного

підходу тісно пов'язане з використанням загальної теорії систем для прийняття управлінських рішень.

Підприємство в рамках даного підходу розглядається як сукупність взаємопов'язаних елементів (підрозділів, функцій, процесів, методів). Основна ідея системної теорії полягає в тому, що будь-яке рішення (дія) має наслідки для всієї системи. Системний підхід в управлінні дозволяє уникнути ситуації, коли прийняте рішення в одній області перетворюється в проблему для іншої.

У рамках системного підходу сформульована модель організації як відкритої системи та дана характеристика зовнішнього середовища як сукупності факторів, що перебувають за її межами, але суттєво впливають на функціонування організації.

Ситуаційний підхід. Системний під хід до управління не дає відповіді на питання про те, чому підприємства з подібним будовою і в одному і тому зовнішньому середовищі (наприклад, працюють в одній галузі та реалізують свою продукцію на одних і тих же ринках), значно відрізняються відносно результату функціонування.

Розв’язати цю проблему намагається ситуаційний підхід за допомогою пов'язання різних прийомів і концепцій з конкретними ситуаціями функціонування підприємства для досягнення своїх цілей. Ситуаційний підхід концентрується на ситуаційних відмінностях між підприємствами і в структурі підприємств та визначає значимі змінні фактори (ситуації) та їх вплив на ефективність діяльності підприємства. Зокрема, встановлені наступні внутрішні змінні: цілі, структура та ресурси організації. Саме варіативність внутрішніх змінних зумовлює можливість вирішення проблеми гнучкості та адаптивності до зовнішнього середовища.

Детальне розроблення ситуаційного підходу управління стало значним внеском у розвиток теорії управління. Цей підхід містить конкретні рекомендації щодо застосування наукових концепцій, принципів та методів залежно від ситуації, що склалася, і умов зовнішнього середовища.

За основу побудови системи управління інформаційною безпекою (СУІБ) підприємства, було обрано як найбільш придатний процесний підхід, що розглядає систему забезпечення інформаційної безпеки як сукупність відповідних процесів.

За суттю, управління інформаційною безпекою (ІБ) - це циклічний процес, що включає декілька процедур, а саме:

- усвідомлення необхідності захисту інформації та постановку завдань;
- збір та аналіз даних про стан ІБ в організації; оцінку інформаційних ризиків;
- планування заходів з обробки ризиків;
- реалізацію і впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів;
- відстеження (моніторинг) функціонування механізмів контролю, оцінку їх ефективності та відповідні коригуючи дії.

Стандартизація у сфері інформаційної безпеки має достатню давню історію. Застосування стандартів у сфері ІБ припустимо в будь-якій організації незалежно від роду її діяльності з метою:

- установлення вимог і цілей в сфері інформаційної безпеки;
- одержання впевненості в тому, що ризики в сфері інформаційної безпеки управляються рентабельно;
- одержання впевненості відповідності діяльності підприємства або організації законодавству та/або іншим нормативним документам;
- реалізації процесу впровадження й управління засобами контролю для одержання впевненості в досягненні специфічних цілей в області захисту організації;
- ідентифікації й відстеження існуючих процесів управління інформаційною безпекою;
- визначення керівництвом організації статусу процесів управління захистом інформації;
- використання внутрішніми й зовнішніми аудиторами для визначення рівня відповідності Політиці безпеки, директивам і стандартам, установленим підприємством/організацією;
- забезпечення партнерів і постачальників відповідною інформацією про стандарти, процедури й політику організації;
- забезпечення споживачів усією відповідною інформацією.

Першим серед стандартів в галузі управління інформаційною безпекою став відомий британський стандарт BS 7799, розроблений (1995) Британським інститутом стандартів (British Standards Institution – BSI). Стандарт BS 7799 складається із двох частин:

Частина 1 «Практичні правила управління інформаційною безпекою» (Part1 Code of Practice for Information Security Management);

Частина 2 «Специфікація системи управління інформаційною безпекою» (Part2 Information Security management — specification for information security management systems).

Вказаний стандарт був обраний за основу для розроблення Міжнародною організацією з стандартизації (ISO) серії стандартів ISO 27001 безпеки й методів управління.

Стандарт ISO 27001 забезпечує єдиний підхід (інакше - уніфікацію процедур) щодо ефективного управління інформаційною безпекою. Заснований на кращих світових практиках, він висуває вимоги до процесів, що забезпечують функціонування системи керування ІБ, їхній постійний моніторинг і поліпшення. Стандарт чітко визначає ключові процеси, якими необхідно управляти при забезпеченні ІБ в організації.

Слід зазначити, що стандарт ISO 27001 узгоджений (гармонізований) зі стандартами систем менеджменту якості ISO 9001: 2000 та ISO 14001: 2004 і базується на їх основних принципах і процесному підході.

При цьому, обов'язкові процедури стандарту якості ISO 9001 також передбачені в стандарті інформаційної безпеки ISO 27001. Структури документації за вимогами вказаних стандартів співпадають. Якщо на

підприємстві вже впроваджена система якості, то можливо констатувати, що значна частина документів, які необхідні відповідно до ISO 27001, може бути вже розроблена та використовується в рамках ISO 9001.

Таким чином, створення на підприємстві системи менеджменту якості відповідно згідно з ISO 9001 або ISO 14001 буде сприяти створення системи управління інформаційною безпекою відповідно до стандарту ISO 27001.

Основними принципами стандарту ISO 27001 є конфіденційність, цілісність та доступність інформації. Керівні принципи поточної версії стандарту охоплюють три головні аспекти: стратегічний, оперативний і дотримання.

Вимоги стандарту фокусуються на наступних проблемах ІБ:

- політика безпеки (Security policy);
- організація інформаційної безпеки (Organization of information security)
- управління ресурсами (Asset management);
- безпека, що обумовлена кадровими ресурсами (Human resources security);
- фізична безпека й безпека оточення (Physical and environmental security);
- управління комунікаціями й процесами (Communications and operations management);
- контроль доступу (Access control);
- придбання, розробка й установлення систем (Information systems acquisition, development and maintenance);
- управління інцидентами інформаційної безпеки (Information security incident management);
- управління безперебійною роботою організації (Business continuity management);
- відповідність правовим і нормативним вимогам (Compliance).

У 2015 році Міжнародною організацією зі стандартизації розроблена і прийнята нова версія стандарту ISO/IEC 27001: 2015. Зміни торкнулися як структури стандарту, так і окремих вимог.

Створення системи управління інформаційною безпекою

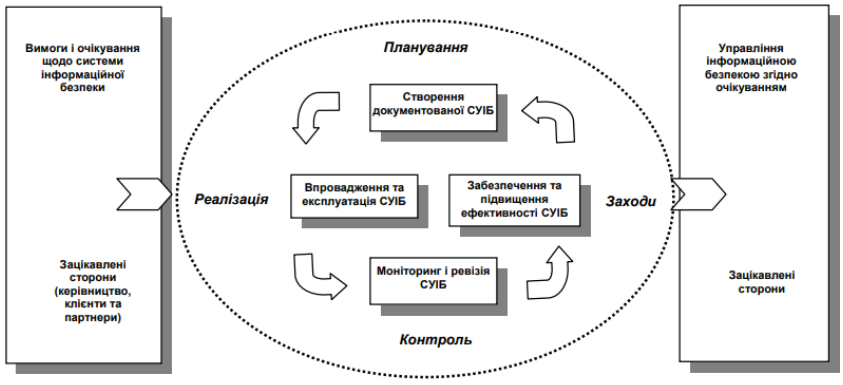


Рис. 14.1. Етапи та процеси створення СУІБ

Створення СУІБ на рис. 14.1 включає циклічний процес «Планування - Реалізація – Контроль – Заходи».

На етапі Планування першим кроком на шляху побудови СУІБ є визначення області її дії. СУІБ може охоплювати всю організацію, окремий

офіс або виділений сервіс, наприклад розробку програмного забезпечення або супровід інформаційної системи.

Формування політики інформаційної безпеки потребує на другому кроці відповіді на запитання:

- чому інформаційна безпека важлива для організації? Які загрози викликають занепокоєння?
- яких цілей у термінах цілісності, конфіденційності й доступності необхідно досягти?
- який рівень ризику є прийнятним для організації?
- які обов'язкові вимоги законодавства повинні враховуватися при побудові СУІБ?

Третій крок цього етапу передбачає заходи щодо оцінки ризику, включаючи вибір методу оцінки ризиків, прийнятний для організації й обраної області дії СУІБ. Для цього необхідно ідентифікувати ризики, включаючи функції:

- визначення ресурсів що захищаються та їх власників;
- виявлення загроз для визначених ресурсів і вразливостей, завдяки яким можлива реалізація загроз;
- встановлення вірогідного впливу на конфіденційність, цілісність та доступність ресурсів.

Оцінка ризиків на цьому кроці здійснюється шляхом:

- з’ясування наслідків для ресурсів в разі реалізації ризиків в плані конфіденційності, цілісності та доступності;
- оцінки імовірності реалізації ризиків;
- встановлення рівня ризиків.

Після завершення оцінки ризиків реалізується процес управління ризиком, наслідком якого має бути ухвалене рішення щодо подальших дій відносно виявлених ризиків.

Існує декілька варіантів дій щодо виявлених ризиків:

- прийняти деякі ризики, що відповідають припустимому рівню СУІБ (наприклад, в випадку, коли втрати від реалізації ризику несуттєві);
- запропонувати механізми контролю для мінімізації ризику;
- адресувати ризики третій стороні, наприклад, завдяки страхуванню.

Також можуть бути застосовані додаткові заходи контролю.

Етап Реалізація (Впровадження). Ця частина циклу передбачає керування механізмами контролю. Для цього необхідна наявність:

- процедури керування інцидентами безпеки (виявлення, оповіщення, відповідальності, аналізу й усунення);
- процедури навчання й «поінформованості» співробітників;
- процедур впровадження, планування й управління необхідними ресурсами.

На цьому етапі здійснюються перевірка досягнення мети, моніторинг вразливостей і недоліків, періодичні оцінки, актуалізація.

Етап Заходи спрямований на усунення виявлених на попередньої частині циклу вразливостей та недоліків, забезпечення та підвищення ефективності СУІБ.

Принципи формування політики безпеки

Як було відзначено вище, під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

Політика безпеки визначає стратегію організації в області інформаційної безпеки, а також пріоритетність вирішення проблем та ресурси, які керівництво вважає за доцільне виділити для цього.

Визначення політики ІБ у загальному випадку (незалежно від виду інформації з обмеженим доступом) повинне зводитися до наступних практичних кроків:

1. Визначення використовуваних керівних документів і стандартів в області ІБ, а також основних положень політики ІБ, включаючи:

- керування доступом до засобів обчислювальної техніки, програм та даних;
- антивірусний захист;
- питання резервного копіювання;
- проведення ремонтних і відбудовних робіт;
- інформування про інциденти в області ІБ.

2. Визначення підходів до керування ризиками: чи є достатнім базовий рівень захищеності або потрібно проводити повний варіант аналізу ризиків.

3. Структуризація контрзаходів по рівнях.

4. Порядок сертифікації на відповідність стандартам в області ІБ.

Політикою ІБ може бути визначена періодичність проведення нарад на рівні керівника з тематики ІБ, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

Для побудови системи захисту інформації необхідно визначити границі системи, для якої повинен бути забезпечений режим інформаційної безпеки. Система керування інформаційною безпекою (система захисту інформації), відповідно, повинна будуватися саме в цих границях.

Опис границь системи, для якої повинен бути забезпечений режим інформаційної безпеки, рекомендується виконувати за наступним планом.

1. Структура організації. Опис існуючої структури й змін, які передбачається внести у зв'язку з розробкою або модернізацією автоматизованої системи обробки інформації.

2. Розміщення засобів обчислювальної техніки, оргтехніки й підтримуючої інфраструктури. Модель ієрархії засобів обчислювальної техніки.

3. Ресурси інформаційної системи, що підлягають захисту. Рекомендується розглянути ресурси автоматизованої системи наступних класів: засоби обчислювальної техніки, дані, системне й прикладне програмне забезпечення. Усі ресурси мають бути оцінені із погляду організації. Для їхньої

оцінки повинна бути обрана система критеріїв і методологія оцінок за цими критеріями.

4. Технологія обробки інформації й розв'язувані завдання. Для розв'язуваних завдань повинні бути побудовані моделі обробки інформації в термінах ресурсів.

У результаті проведення робіт повинен бути створений документ, у якому:

- зафіксовані границі й структура системи;
- перераховані ресурси, що підлягають захисту;
- дана система критеріїв для оцінки їх цінності.

Мінімальним вимогам до режиму інформаційної безпеки відповідає базовий рівень. Звичайною областю використання цього рівня є типові проектні рішення. Існує ряд стандартів і специфікацій, у яких розглядається мінімальний (типовий) набір найбільш імовірних загроз, таких як віруси, збої встаткування, несанкціонований доступ і т.д.

Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від імовірності здійснення загроз і уразливості ресурсів. Таким чином, характеристики загроз на базовому рівні розглядати не обов'язково.

У випадку, коли порушення інформаційної безпеки чреваті важкими наслідками, базовий рівень вимог до режиму інформаційної безпеки є недостатнім. Для того, щоб сформулювати додаткові вимоги, необхідно:

- визначити цінність ресурсів;
- до стандартного набору додати список загроз, актуальних для досліджуваної інформаційної системи;
- оцінити ймовірності загроз;
- визначити рівень вразливості ресурсів.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані, стратегія захисту визначена, тоді складається програма, реалізація якої повинна забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми й т.п.

Існують різні підходи до оцінки ризиків. Вибір підходу залежить від рівня вимог, пропонованих в організації до режиму інформаційної безпеки, характеру прийнятих в увагу загроз (спектра впливу загроз) і ефективності потенційних контрзаходів.

Процес оцінки ризиків включає кілька кроків.

1. Ідентифікація ресурсу й оцінювання його кількісних показників (визначення негативного впливу).
2. Оцінювання загроз.
3. Оцінювання вразливостей.
4. Оцінювання існуючих і перспективних засобів забезпечення.
5. Оцінка ризиків.

На підставі оцінки ризиків вибираються засоби, що забезпечують необхідний рівень ІБ.

Ресурси, значимі для нормальної роботи організації, що й мають певний ступінь уразливості, уважаються підданими ризику, якщо стосовно них існує яка-небудь загроза. При оцінюванні ризиків ураховуються потенційні негативні впливи від небажаних подій і показники значимості розглянутих уразливостей і загроз для цих ресурсів.

Ризик характеризує небезпека, якої може зазнати система, що й використовує її організація.

Ціль оцінки ризиків полягає у визначенні характеристик ризиків для інформаційної системи і її ресурсів. На основі таких даних можуть бути обрані необхідні засоби керування ІБ.

Ризик залежить від показників цінності ресурсів, імовірності реалізації загроз для ресурсів і ступеня легкості, з якого уразливості можуть бути використані при існуючих або планованих засобах забезпечення інформаційної безпеки. Таким чином, при оцінюванні ризиків ураховуються:

- цінність ресурсів;
- оцінка значимості загроз;
- ефективність існуючих і планованих засобів захисту.

Показники ресурсів або потенційний негативний вплив на діяльність організації можна визначати декількома способами:

- кількісними (наприклад, вартісні);
- якісними (можуть бути побудовані на використанні таких понять, як, помірний, середній або надзвичайно небезпечний);
- комбінацією двох попередніх.

Для того, щоб конкретизувати визначення ймовірності реалізації загрози, розглядається певний відрізок часу, протягом якого передбачається захистити ресурс. Імовірність того, що загроза реалізується, визначається наступними факторами:

- привабливість ресурсу як показник при розгляді загрози від навмисного впливу з боку людини;
- можливість використання ресурсу для одержання прибутку як показник при розгляді загрози від навмисного впливу з боку людини;
- технічні можливості загрози, використовувані при навмисному впливі з боку людини;
- імовірність того, що загроза реалізується;
- ступінь легкості, з якого уразливість може бути використана.

Питання про те, як провести границю між припустимими й неприпустимими ризиками, вирішується користувачем. Очевидно, що розробка політики безпеки вимагає обліку специфіки конкретних організацій.

На підставі політики безпеки будується програма безпеки, яка реалізується на процедурному й програмно-технічному рівнях.

Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001

Створена на підприємстві СУІБ потребує перевірки щодо правильності її реалізації відповідно до вимог стандартів. Процедура перевірки на відповідність стандартам отримала назву сертифікація.

Перевагами проведення сертифікації на відповідність стандарту ISO/IEC 27001 є:

- незалежне підтвердження того, що система внутрішнього контролю та управління безпекою відповідають бізнес-задачам організації та забезпечують необхідні ефективність і безперервність виробництва;

- демонстрація партнерам і клієнтам можливості виконання контрактних зобов'язань і прихильності фірми до захисту інформації;

- об'єктивно підтвердження того, що ризики компанії в області ІБ належним чином визначені, оцінені і управляються на основі процесного підходу;

- забезпечення актуальності системи захисту за рахунок регулярних перевірок, постійного моніторингу системи менеджменту та її послідовного вдосконалення.

Сертифікація проводиться уповноваженими світовими організаціями, зокрема, це стосується, зокрема, BSI - Британського інституту стандартів, експертної організації Бюро Верітас (Bureau Veritas Certification Holding SAS), міжнародного концерну з надання аудиторських послуг ТЮФ Райнланд Груп (TÜV Rheinland Group), їх регіональних представництв та інших органів з сертифікації, що акредитовані встановленим порядком.

Для отримання та підтримки сертифікації замовники цих послуг повинні розробити і підтримувати в робочому стані свої системи менеджменту відповідно до вимог, що встановлені специфікаціями, забезпечуючи вільний доступ органів з сертифікації до зазначених систем менеджменту з метою проведення аудиту, чи іншої перевірки їх функціонування відповідно до цих специфікацій.

У загальному випадку процес сертифікаційного аудиту, що проводиться, наприклад, BSI може включати наступні процедури:

- Необов'язковий попередній аудит;

- Сертифікаційний аудит, що включає:

• Аудит документації з наданням часу на усунення невідповідностей (до3 місяців);

• Аудит функціонування та впровадження СУІБ: обстеження системи та опитування співробітників з наданням рекомендації щодо усунення невідповідностей, сертифікація в разі виявлення незначних невідповідностей;

• Усунення невідповідностей (6-12 місяців);

- Ухвалення рішення про сертифікацію підприємства;

- Інспекційний аудит (1 раз на рік);

- Повторна-сертифікація через 3 роки.

Переважно, замовниками процедур сертифікації на відповідність вимогам стандарту є компанії з IT інфраструктурою, що динамічно розвивається, та в яких реалізація ризиків може призвести до значних фінансових втрат.

ТЕМА 12. Методика побудови комплексних систем захисту інформації в автоматизованих системах

Комплексні системи захисту

Відповідно до законодавства України забезпечення в автоматизованій системі (АС) захисту інформації з обмеженим доступом (ІзОД) та іншої інформації, захист якої гарантується державою, полягає у створенні комплексної системи захисту інформації (КСЗІ) як невід'ємної складової компоненти АС і яка являє собою сукупність організаційних та інженерно-технічних заходів, програмно-технічних засобів, що забезпечують необхідний рівень захисту інформації на протязі усього життєвого циклу АС.

Для створення КСЗІ необхідно провести комплекс таких робіт:

- провести класифікацію інформації, що буде накопичуватися та оброблятися в АС, за правовим режимом та за режимом доступу;
- провести аналіз середовищ функціонування АС (інформаційного, технологічного, середовища користувачів, середовища потенційних порушників);
- розробити модель загроз для інформації з врахуванням конкретних умов експлуатації АС та модель потенційних порушників;
- на підставі розроблених моделей розробити політику безпеки інформації, визначити специфікації функціональних послуг захисту інформації від несанкціонованого доступу та вимоги з захисту інформації від витоку технічними каналами. Всі ці вимоги мають бути включені до технічного завдання (ТЗ) на створення АС або до окремого ТЗ на створення КСЗІ;
- визначити механізми та заходи захисту, необхідні для реалізації вимог технічного завдання і забезпечити їх впровадження на об'єкті;
- забезпечити проведення експертизи захищеності інформації в АС відповідно до Положення про державну експертизу у сфері технічного захисту інформації.

Розробка КСЗІ у АС виконується згідно вимог технічного завдання на розробку КСЗІ. Технічне завдання є засадничим організаційно-технічним документом для виконання робіт по забезпеченню захисту інформації в АС.

Створення систем захисту інформації здійснюється відповідно до вимог нормативних документів системи технічного захисту інформації (НД ТЗІ) та з урахуванням положень стандартів, включаючи серію міжнародних стандартів ISO/IEC 27001, та передбачає реалізацію наступних етапів:

- проведення аудиту об'єкту інформаційної діяльності.
- створення Моделі загроз.
- аналіз та оцінка ризиків.
- розробка Політики безпеки.
- проектування системи захисту.
- розробка організаційних та нормативно-технічних документів.
- випробування та дослідна експлуатація системи.

Системне забезпечення й основні принципи побудови захисту інформації

Як вже відмічалося вище, для забезпечення інформаційної безпеки на основі політики інформаційної безпеки складається програма забезпечення безпеки інформації. Програма забезпечення безпеки має на меті побудову системи захисту інформації.

Захист інформації повинен ґрунтуватися на наступних основних принципах:

- системності;
- комплексності;
- безперервності захисту;
- розумної достатності;
- гнучкості керування й застосування;
- відкритості стандартів алгоритмів і механізмів захисту;
- простоти застосування захисних заходів і засобів.

Системний підхід до захисту інформаційних ресурсів припускає необхідність обліку всіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння й розв'язку проблеми забезпечення безпеки.

При створенні системи захисту необхідно враховувати всі слабкі, найбільш уразливі місця інформаційної системи, а також характер, можливі об'єкти й напрями атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в розподілені системи та несанкціонованого доступу (НСД) до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення й НСД до інформації, але й зважаючи на можливість появи принципово нових шляхів реалізації загроз безпеки.

У розпорядженні фахівців з безпеки є широкий спектр заходів, методів і засобів захисту. Комплексне їхнє використання припускає погоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації загроз і не припускаючи слабких місць на стиках окремих її компонентів.

Система захист повинна будуватися за методом ешелонування, із створенням декількох рубежів протидії спробам атакувати систему, забезпечуючи так званий багаторівневий захист. Убезпечення зовнішнього периметру в цьому випадку забезпечується інженерно-технічними засобами, організаційними й правовими заходами.

Прикладний рівень захисту, що враховує особливості предметної області, представляє внутрішній рубіж оборони.

Захист інформації – це не разовий захід і, навіть, не певна сукупність проведених заходів і встановлених засобів захисту, а безперервний цілеспрямований процес, що припускає впровадження відповідних заходів на всіх етапах життєвого циклу інформаційної системи, починаючи із самих ранніх стадій проектування, а не тільки на етапі її експлуатації.

Розробку системи захисту доцільно проводити паралельно з створенням самої системи, яка захищається. Це забезпечує врахування вимог з безпеки вже під час проектування архітектури АС й, в остаточному підсумку, дозволяє

створити більш ефективні (як по витратах ресурсів, так і по стійкості) захищені системи.

Більшість програмних та технічних засобів захисту потребує організаційної підтримки, регулярної оцінки стану та адміністрування для ефективного виконання функцій за призначенням, наприклад, своєчасної зміни імен, паролів, ключів шифрування та забезпечення їх належного зберігання і застосування, змін повноважень користувачів тощо.

Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу застосованих методів і засобів захисту, або впровадження спеціальних програмних і апаратних «закладок», або інших засобів подолання системи захисту після відновлення її функціонування.

Створити абсолютно неперебoрну систему захисту принципово неможливо. За умов необмеженого часу та достатніх коштів практично можна подолати будь-який захист.

Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки. Високоефективна система захисту коштує дорого, використовує при роботі істотну частину потужності й ресурсів і може створювати відчутні додаткові незручності користувачам.

Важливо правильно вибрати той достатній рівень захисту, завдяки якому витрати, ризик і розмір можливого збитку були б прийнятними (завдання аналізу ризику).

Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому вжиті заходи й встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнем захищеності, засобу захисту повинні мати певну гнучкість.

Особливо важливою ця властивість є в тих випадках, коли установку засобів захисту необхідно здійснювати на працюючу інформаційну систему, не порушуючи процесу її нормального функціонування.

Крім того, зовнішні умови й вимоги із часом міняються. У таких ситуаціях властивість гнучкості рятує власників інформаційної системи від необхідності вживання кардинальних заходів щодо повної заміні засобів захисту на нові.

Суть принципу відкритості стандартів алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок секретності організації захисту, структури системи захисту та алгоритмів функціонування її підсистем.

Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання, навіть розробникові. Однак, це зовсім не означає, що інформація про конкретну систему захисту повинна бути загальнодоступна.

Механізми захисту повинні бути інтуїтивно зрозумілі й прості у використанні. Застосування засобів захисту не повинне бути зв'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових працезатрат при звичайній роботі легальних користувачів, а також не повинне

вимагати від користувача виконання рутинних малозрозумілих йому операцій (наприклад, уведення декількох паролів і імен і т.д.).

Етапи створення комплексної системи захисту інформації

Організація та порядок виконання робіт із захисту інформації у АС – це порядок прийняття рішень щодо складу комплексної системи захисту інформації кожного з вузлів АС в залежності від умов їх функціонування і видів оброблюваної інформації, визначення обсягу і змісту робіт, їх етапності, основних завдань та порядку виконання робіт кожного етапу відповідно до вимог законодавства України, а також нормативних документів у сфері технічного та криптографічного захисту інформації.

Порядок створення КСЗІ є єдиним незалежно від того, створюється КСЗІ в елементах (підсистемах) в АС, які проектуються, чи в діючих елементах АС.

В рамках заходів із формування вимог до системи захисту та проектування системи захисту виконуються наступні заходи:

- проведення обстеження АС;
- формування завдання (вихідних вимог) на створення КСЗІ;
- розробка моделі загроз інформації та політики безпеки;
- створення плану захисту;
- розроблення технічного завдання на створення КСЗІ в АС;
- погодження розробленого технічного завдання з Державною службою спеціального зв'язку та захисту інформації України.

Розглянемо більш детально перші три заходи.

Обстеження АС

Передбачається, що під час виконання цих робіт АС розглядається як організаційно-технічна система, що поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування АС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування АС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах виконання робіт.

Перелік робіт може бути уточнений виконавцем та погоджений замовником робіт на етапі розроблення технічного проекту АС.

Формування завдання (вихідних вимог) на створення КСЗІ

На етапі формування вихідних вимог на створення КСЗІ виконуються наступні процедури:

- визначаються завдання захисту інформації в АС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту;
- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ в АС, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, інші обмеження щодо середовищ функціонування АС, обмеження щодо використання ресурсів АС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ.

Розробка моделі загроз інформації

Модель загроз інформації в АС - це опис методів та засобів реалізації загроз для інформації в конкретних умовах функціонування автоматизованої системи.

Процес формування моделі загроз інформації є одним з ключових факторів забезпечення безпеки АС, оскільки її вибір безпосередньо впливає на визначення конкретного переліку послуг безпеки та необхідних заходів і засобів захисту, що мають бути застосовані в системі.

Всебічність та повнота аналізу загроз дає необхідну впевненість, що враховано всі суттєві загрози безпеки інформації.

Конструктивним шляхом створення моделі загроз є формування окремих моделей загроз для кожного типового компоненту системи (зокрема для локально обчислювальних мереж підрозділів, вузла Інтернет, вузлів зв'язку з Інтернет, каналів зв'язку і вузлів зв'язку з підрозділами) та типових об'єктів захисту (робочих станцій, серверів, мережевого обладнання локальнообчислювальних мереж (ЛОМ) обробки даних, ЛОМ прийняття рішень тощо).

Формування окремих моделей загроз повинно здійснюватись на підставі загальної класифікації загроз інформації та відповідної моделі загроз, а також загальної моделі порушника

У зв'язку можливістю модернізації та розвитку АС протягом всьогоі життєвого циклу АС модель загроз необхідно переглядати, а також з удосконаленням технічних та програмних засобів подолання механізмів захисту.

Під час створення моделі загроз виконується оцінка, у процесі здійснення якої, фахівці у галузі інформаційної безпеки одержують інформацію для її використання на всіх наступних етапах побудови комплексної системи забезпечення інформаційної безпеки. А саме:

- класифікація та опис ресурсів АС (операційних систем, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т. ін.);
- аналіз інформаційної моделі існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС;
- визначення переліку загроз і можливих каналів витоку інформації;
- визначення послуг безпеки, які треба реалізувати;
- визначення вимог до організаційно-технічних, нормативно-правових та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту;
- прийняття остаточного рішення про склад КСЗІ.

Формування політики (основних правил) безпеки інформації

В цілому підходи щодо формування Політики безпеки інформації які визначені у НД ТЗІ та стандарті ISO/IE 27001 (викладенні у попередньому розділі) у цілому співпадають.

Звернемо увагу лише на уточнення окремих формулювань. Політика безпеки інформації є сукупністю законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації в АС та спрямовані на захист інформації від впливу реалізації визначених загроз.

Політика безпеки повинна визначати ресурси, що потребують захисту. Мають бути визначені загрози для інформації і вимоги до захисту від цих загроз.

Кожен користувач, а також адміністратори та особи, яких призначено відповідальними за безпеку інформації, мають бути ознайомлені з положеннями політики безпеки в частині, що їх стосується, і нести персональну відповідальність за додержання цих положень.

Політика безпеки повинна встановлювати функціональні обов'язки керівників, користувачів, адміністраторів і осіб, яких призначено відповідальними за безпеку інформації.

Політика інформаційної безпеки являє собою головний нормативний документ, який затверджується керівництвом власника АС. Документ розробляється з урахуванням особливостей діяльності органу (підприємства, організації), його організаційної структури, розміщення та структури корпоративної інформаційної системи й характеру розв'язуваних завдань.

Політика безпеки описує питання забезпечення безпеки у всіх областях діяльності органу (підприємства) й на всіх ділянках корпоративної інформаційної системи:

- на кожному окремому об'єкті (центральний офіс, підрозділи, регіональні філії);
- при взаємодії між підрозділами;
- під час контактів з з партнерами або клієнтами;
- при використанні ресурсів відкритих мереж.

Політика забезпечення інформаційної безпеки повинна включати наступні основні розділи:

- основні цілі й напрямки забезпечення інформаційної безпеки корпоративної інформаційної системи;
- основні загрози інформаційної безпеки органу (підприємства), способи їхньої реалізації й можливі види збитку;
- необхідні заходи, методи й засоби забезпечення інформаційної безпеки корпоративної системи (організаційні, програмно-технічні, фізичні);
- порядок організації робіт із забезпечення інформаційної безпеки корпоративної інформаційної системи.

Розроблення технічного завдання на створення КСЗІ в АС

Технічне завдання на створення КСЗІ АС є основним організаційнотехнічним документом, який визначає вимоги із захисту

оброблюваної в АС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі АС.

ТЗ на створення КСЗІ розробляється на відповідній стадії робіт зі створення АС, яка визначається ТЗ на створення АС, з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ мають бути викладені вимоги до функціонального складу, порядку розробки і впровадження технічних та програмних засобів, що забезпечують безпеку інформації в процесі її оброблення в АС.

Додатково можуть бути викладені вимоги до організаційно-технічних, нормативно-правових та інших заходів захисту, що реалізуються поза АС у доповнення до комплексу програмних та програмно-апаратних засобів захисту інформації.

Розроблення та оформлення ТЗ на КСЗІ, його зміст, порядок погодження та затвердження повинні відповідати вимогам нормативно-правових актів та нормативних документів у сфері технічного захисту інформації.

Технічне завдання на розробку КСЗІ в випадку службової інформації або державної таємниці має бути погоджене Держспецзв'язку України.

Проект технічного завдання повинен бути включати наступні розділи:

- загальні вимоги щодо створення комплексної системи захисту інформації в АС;
- перелік і вимоги до нормативних документів, які необхідно розробити і погодити при побудові КСЗІ та для здійснення повсякденної роботи АС;
- перелік етапів зі створенню КСЗІ;
- перелік устаткування й програмних засобів для створення КСЗІ;
- термін виконання робіт по створенню КСЗІ.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної інформаційної підмережі як розширений, так і скорочений.

У якості системи захисту базової програмної платформи для розробки АС можуть бути використані апаратні та програмні засоби, що мають експертні висновки (сертифікати відповідності) Держспецзв'язку України , наприклад, такі програмні засоби захисту інформації від несанкціонованого доступу як «Гриф», «Лоза», «Рубіж» тощо.

Склад засобів захисту може бути уточнений виконавцем та погоджений із замовником робіт на етапі розроблення технічного проекту.

Комплекс засобів захисту інформації

Засоби захисту розміщуються в межах контрольованої території, у визначеному замовником спеціалізованому приміщенні (апаратній залі) разом з іншим телекомунікаційним обладнанням або окремо.

Маскування топології взаємодіючих мереж, автентифікація користувачів та ресурсів, управління зовнішнім доступом до ресурсів локальної мережі досягається шляхом розроблення та впровадження КСЗІ з використанням

міжмережевих екранів, засобів криптографічного захисту інформації, впровадження організаційно-технічних (нормативно-розпорядчих) заходів, створенням відповідних інструкцій, а також завдяки настроювання та конфігурування операційних систем та відповідного програмного забезпечення.

Захист трафіку поза межами контрольованої зони, включаючи з'єднання клієнтів з серверами додатків (баз даних) забезпечується шляхом шифрування інформаційного обміну або створення віртуальних приватних мереж VPN (Virtual Private Network) із застосуванням засобів криптографічного захисту інформації, що мають експертний висновок.

Зазвичай, за допомогою таких засобів забезпечується конфіденційність і цілісність даних, що передаються каналами зв'язку.

Залежно від виду інформації використовуються програмні (конфіденційна інформація) або апаратні (службова, державна таємниця) апаратні засоби.

Під час створення КСЗІ доцільно використовується модульний принцип її побудови, що надасть можливість нарощення та модернізації системи без порушення політики безпеки та загальної працездатності системи.

Вимоги до організаційних заходів

Організаційні заходи є невід'ємною частину КСЗІ, оскільки не лише дозволяють запобігати загрозам безпеки інформації та блокувати їх певну частину, а також поєднувати в єдину систему усі засоби захисту.

Для безпосередньої організації робіт із створення і ефективного функціонування КСЗІ має бути створений або визначений наказом керівника підрозділ - служба захисту інформації (СЗІ) в АС.

Для врегулювання питань діяльності СЗІ на підприємстві наказом керівника вводиться в дію Положення про СЗІ. Це Положення розробляється майбутнім власником АС під час її створення. В загальному випадку Положення повинно складатись з таких розділів:

- загальні положення;
- завдання служби захисту інформації;
- функції служби захисту інформації;
- повноваження і відповідальність служби захисту інформації;
- взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми підприємствами та установами;
- штатний розклад та структура служби захисту інформації;
- організація робіт служби захисту інформації;
- фінансування служби захисту інформації.

СЗІ має виступати організатором та/або виконавцем робіт у галузі захисту інформації в частині управління КСЗІ, управління доступом, реєстрації та обліку носіїв, резервного копіювання та архівування програмного забезпечення та даних системи захисту.

Організаційні заходи щодо управління КСЗІ повинні передбачати реалізацію наступних процесів:

- регламентацію порядку дій користувачів щодо додержання прийнятої політики безпеки;

- визначення порядку контролю за додержанням політики безпеки, розслідування фактів порушень та прийняття заходів щодо усунення їх наслідків та недопущення повторних випадків;

- встановлення порядку проведення модернізації АС (у тому числі. інсталяції оновлень системного і прикладного програмного забезпечення), а також здійснення контролю за цими процесами;

- розробку організаційно-методичних та розпорядчих документів, що регламентують порядок і правила функціонування КСЗІ (включаючи проекти наказів та інструкції, плани роботи, графіки контролю та проведення регламентних робіт тощо).

В плані управління доступом організаційні заходи повинні передбачати:

- встановлення порядку розподілу атрибутів розмежування доступу;

- визначення порядку доступу користувачів до АРМ, носіїв інформації та його контролю;

- врегулювання умов доступу до ресурсів та засобів АС під час проведення ремонтних та регламентних робіт, технічного забезпечення АС, включаючи санкціонування відповідних заходів, розгляд і документальне затвердження змін.

Організаційні заходи щодо реєстрації та обліку носіїв включають наступні процедури:

- встановлення порядку обліку, видачі, використання і зберігання змінних носіїв інформації, що містять еталонні і резервні копії;

- визначення порядку організації зберігання, використання і знищення документів і носіїв із ІзОД;

- визначення порядку обліку технічних засобів АС.

Організаційні заходи з резервного копіювання та архівування програмного забезпечення та даних повинні передбачати:

- розробку регламенту та впровадження технології резервного копіювання інформації в АС та ведення архівів;

- розробку порядку відновлення зарезервованої інформації у відповідності до її грифу;

- розробку схеми ротації носіїв.

Склад проектної та експлуатаційної документації

Обсяг проектної та експлуатаційної документації на КСЗІ визначається державними стандартами на проектування автоматизованих систем. Склад документації може уточнюватися за згодою замовника та виконавця в процесі виконання відповідних дослідних-конструкторських робіт.

Необхідно мати на увазі, що недостатній обсяг документації може суттєво ускладнювати сертифікацію або експертизу систем, а також їх експлуатацію.

В загальному випадку проектна документація на систему повинна включати:

- технічний проект інформаційної системи;

- робочу документацію;

- класифікацію інформації;

- класифікацію користувачів за рівнем повноважень та місцем їх розміщення;

- загальний опис системи;

- модель загроз безпеці інформації та модель потенційних порушників;

- опис політики безпеки інформації;

- план технічного захисту;

- опис технічних засобів захисту.

До складу експлуатаційної документації на систему включаються:

- накази: про створення комісії з обстеження АС, про створення комісії з категоріювання АС, про створення СЗІ, призначення адміністратора безпеки та інших адміністраторів, про створення комісії з проведення попередніх випробувань КСЗІ, про проведення дослідної експлуатації;

- акти: категоріювання АС, обстеження АС, про передачу КСЗІ в дослідну експлуатацію, завершення дослідної експлуатації;

- програма та методика випробувань;

- протокол попередніх випробувань КСЗІ;

- журнал навчання користувачів;

- політика безпеки;

- положення про службу захисту інформації в АС;

- план захисту інформації в АС;

- інструкції: із забезпечення режиму безпеки при роботі в АС, з порядку забезпечення антивірусного захисту інформації, користувача в АС, адміністратора безпеки, системного адміністратора, з тестування системи, з виконання регламентних та ремонтних робіт, про порядок введення в експлуатацію КСЗІ, про порядок модернізації КСЗІ;

- паспорт-формуляр на АС.

Склад та зміст плану захисту інформації визначається СЗІ згідно з НД ТЗІ 1.4-001-2000.

Інструкція користувача повинна включати короткий опис механізмів захисту та інструкції щодо порядку роботи з ними в процесі взаємодії користувача з АС.

Інструкція адміністратора безпеки призначена для забезпечення виконання функціональних обов’язків адміністратора безпеки (персоналу СЗІ) і повинна включати описи:

- дій щодо управління захистом (встановлення атрибутів доступу, прав, порядок надання користувачам особистих ідентифікаторів та паролів тощо.);

- процедур роботи із засобами реєстрації;

- процедур інсталяції засобів захисту інформації;

- процедур оперативного відновлення працездатності КСЗІ після збоїв.

Інструкція системного адміністратора повинна описувати дії щодо адміністрування АС, такі як:

- процедури супроводження програмного забезпечення компонентів АС, перевірки його цілісності та працездатності;

- процедури інсталяції, генерації і запуску засобів адміністрування АС та мережевого обладнання;

- процедури перевірки працездатності засобів адміністрування;
- опис процедур оперативного відновлення працездатності після збоїв.

Документація техно-робочого проекту повинна містити основні проектні і технічні рішення щодо побудови АС (компонентів АС). Склад та зміст документації повинен відповідати вимогам державних стандартів, у тому числі в частині виготовлення конструкторської документації - стандартам Єдиної системи конструкторської документації (ЄСКД), в частині виготовлення експлуатаційної документації - ГОСТ 34.201.

Склад та зміст опису компонентів КСЗІ та інструкцій користувача і адміністратора безпеки повинні відповідати вимогам НД ТЗІ 2.5-004-99.

Остаточний склад експлуатаційної документації виконавець робіт погоджує з замовником за результатами дослідної експлуатації КСЗІ АС.

Випробування та дослідна експлуатація

Завершена КСЗІ підлягає попереднім випробуванням. Порядок підготовки та проведення випробувань має відповідати нормативним документам ГОСТ 34.603-92.

Метою попередніх випробувань є перевірка працездатності КСЗІ, встановлення відповідності досягнутого в АС рівня захищеності інформації вимогам цього технічного завдання та визначення можливості прийняття її у дослідну експлуатацію.

Також під час випробувань перевіряється відповідність КСЗІ вимогам що встановлені в ТЗ.

Обсяг випробувань має бути достатнім для вичерпної оцінки коректності реалізації усіх вимог захисту інформації. Обсяг випробувань визначається документом “Програма та методика випробовувань”, який готується виконавцем робіт та погоджується із замовником. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

У ході випробувань КСЗІ повинно бути перевірено функціонування всіх її програмно-технічних компонент і наявних в них механізмів захисту на відповідність вимогам, які пред’являються до них в ТЗ на КСЗІ, а також достатність впроваджених в АС організаційних та інших заходів із захисту інформації.

Перевірка програмно-технічних компонент КСЗІ повинна включати випробовування засобів керування доступом, засобів реєстрації та обліку, засобів забезпечення цілісності інформації, засобів керування КСЗІ.

Випробування повинні проводитись з використанням даних, які не містять ІзОД.

Попередні випробування організовує замовник АС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником АС створюється комісія, головою якої призначається представник замовника. За погодженням до складу комісії залучаються представники замовника.

Результати попередніх випробувань оформлюються “Протоколом випробувань”, що повинен містити висновок щодо можливості прийняття КСЗІ

у дослідну експлуатацію. У висновках вказуються також перелік виявлених недоліків, необхідні заходи з їх усунення та рекомендовані терміни виконання цих робіт.

Після усунення недоліків (у випадку їх наявності) та коригування проектної, робочої і експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

Основними задачами під час дослідної експлуатації КСЗІ є:

- відпрацювання технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів АС та автоматизованого контролю за діями користувачів;

- навчання співробітників СЗІ та користувачів АС, набуття ними практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоєння вимог організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

- за необхідністю доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування комплексу засобів захисту та відповідного коригування робочої та експлуатаційної документації.

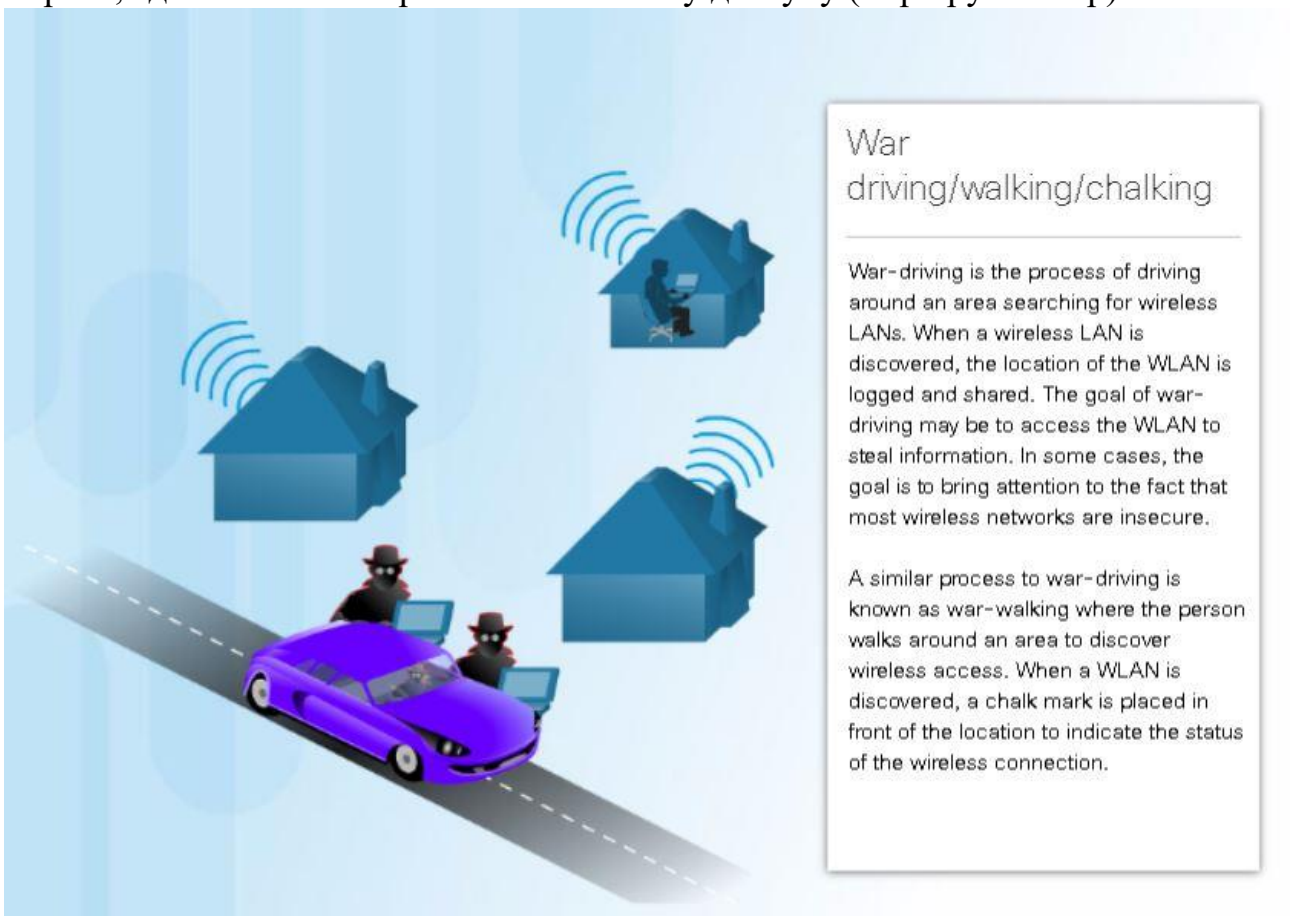
За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

ТЕМА 13. Безпека бездротових мереж

Чому хакери цілять в бездротову приватну мережу?

Однією з основних переваг бездротової мережі є легкість та зручність підключення пристроїв. На жаль, така легкість підключення і той факт, що інформація передається через повітря, також робить таку мережу вразливою для перехоплення та нападів, як показано на рис 1. Перед розгортанням бездротової мережі важливо розглянути, як планується захистити доступ до неї.

За допомогою бездротового з'єднання атакуючий не потребує фізичного підключення до комп'ютера у мережі або будь-якого з пристроїв для доступу до такої мережі. Зловмисник може налаштувати отримання сигналів з бездротової мережі, здійснивши настроювання на точку доступу (маршрутизатор).



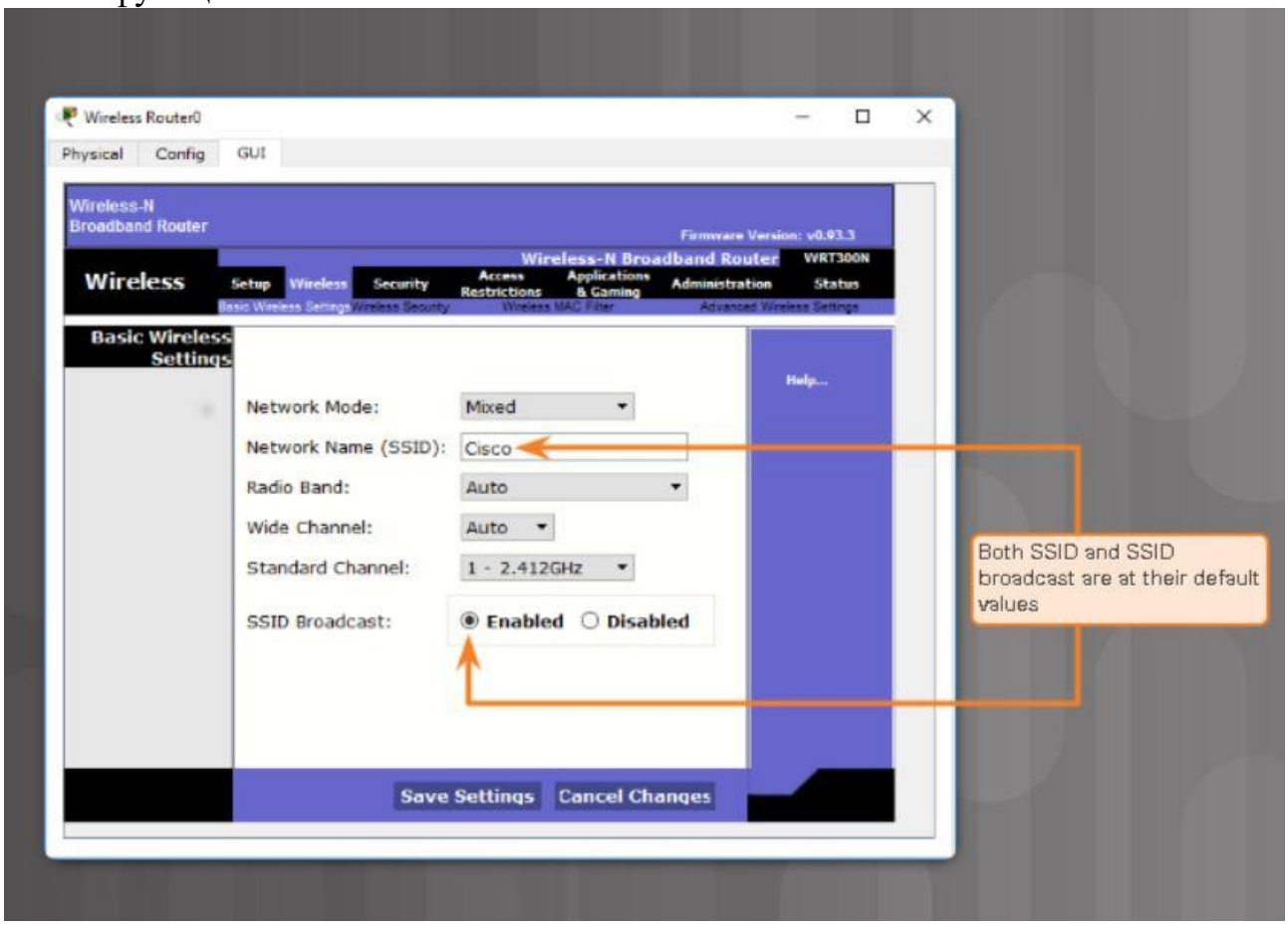
Зловмисник може отримати доступ до приватної мережі (англ. PAN) з будь-якого місця, до якого досягає бездротовий сигнал. Після того, як акакуючі матимуть доступ до приватної мережі, вони можуть безкоштовно користуватися Інтернет-службами, за які сплачено власником PAN, а також мати доступ до комп'ютерів у мережі, щоб пошкодити файли, або викрасти особисту та приватну інформацію.

Ці вразливості в бездротових мережах вимагають спеціальних функцій безпеки та методів реалізації, щоб захистити WLAN від атак. До них відносяться прості кроки під час первинної настройки бездротового пристрою, а також більш просунуті конфігурації безпеки.

Трансляція SSID

Один з простих способів отримати доступ до бездротової мережі - це ім'я мережі або SSID.

Усі комп'ютери, підключені до бездротової мережі, повинні знати SSID. За замовчуванням, бездротові маршрутизатори та точки доступу передають SSID всім комп'ютерам в межах бездротового діапазону. Якщо активація широкомовної передачі SSID активована, як показано на рис. 2, будь-який бездротовий клієнт може виявити мережу та підключитися до неї, якщо немає інших функцій безпеки.

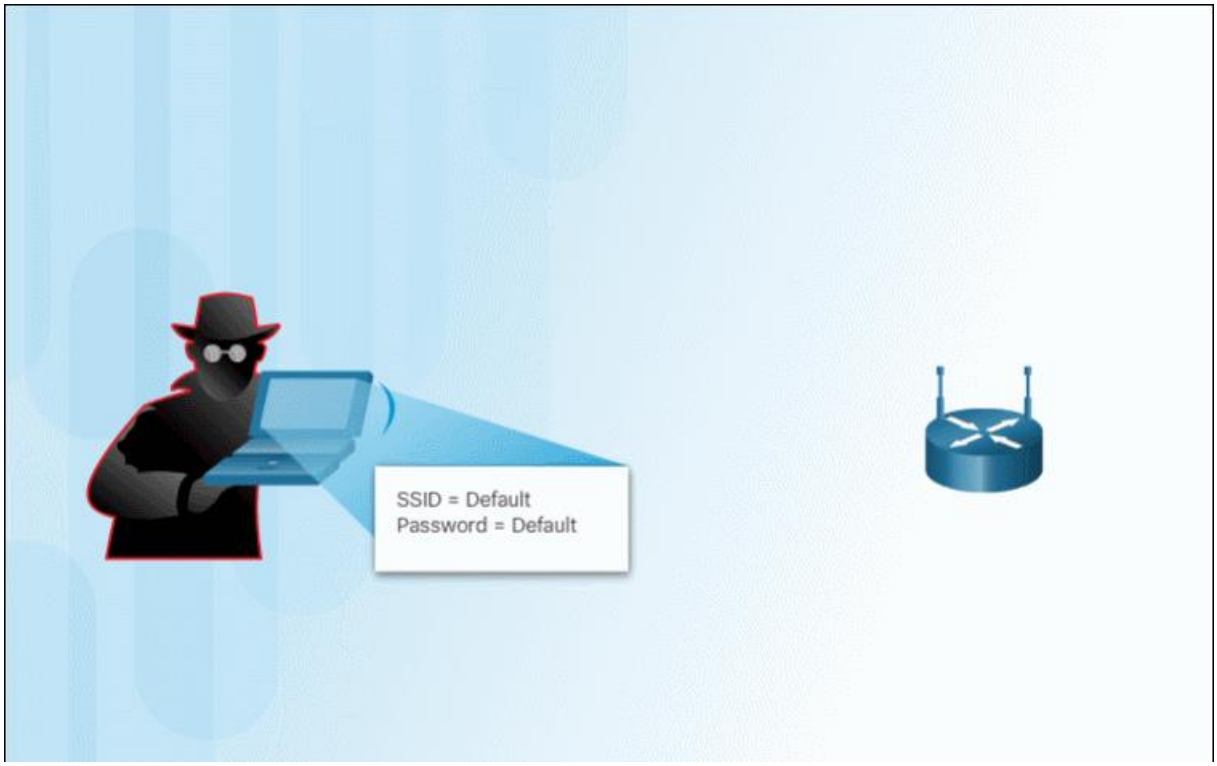


Функцію трансляції SSID можна вимкнути. Коли вона вимкнена, той факт, що ця мережа існує, більше не оприлюднюється. Будь-який комп'ютер, який намагається підключитися до мережі, повинен вже знати SSID. Відключення єдиної передачі SSID не захищає бездротову мережу від досвідчених хакерів. SSID можна визначити шляхом захоплення та аналізу пакетів бездротового зв'язку, якими обмінюються клієнти та точка доступу. Навіть якщо трансляція SSID вимкнена, хтось може потрапити до такої мережі за допомогою відомого стандартного SSID. Окрім того, якщо інші параметри за замовчуванням, такі як паролі та IP-адреси, не змінюються, хакери можуть отримати доступ до ОС та самостійно внести зміни. Інформація за замовчуванням повинна бути змінена на щось більш безпечне та унікальне.

Зміна параметрів за замовчуванням

Які налаштування за замовчуванням і чому вони там? Більшість бездротових точок доступу та маршрутизаторів попередньо настроєні з такими параметрами, як SSID, паролі адміністратора та IP-адреси. Ці налаштування полегшують користувачу-початковцю налаштовувати пристрій у середовищі

приватної мережі. На жаль, ці налаштування за замовчуванням також дозволяють зловмиснику легко ідентифікувати та проникнути в мережу (рис. 3).



Зміна налаштувань за замовчуванням на бездротовому маршрутизаторі не захистить мережу сама по собі. Наприклад, ідентифікатори SSID передаються як відкритий текст. Є пристрої, які будуть перехоплювати бездротові сигнали та читати текстові повідомлення. Навіть якщо трансляція SSID вимкнена та змінені значення за замовчуванням, зловмисники можуть дізнатися назву бездротової мережі шляхом використання пристроїв, які перехоплюють сигнали бездротового зв'язку. Ця інформація буде використовуватися для підключення до мережі. Для захисту WLAN використовується декілька методів.

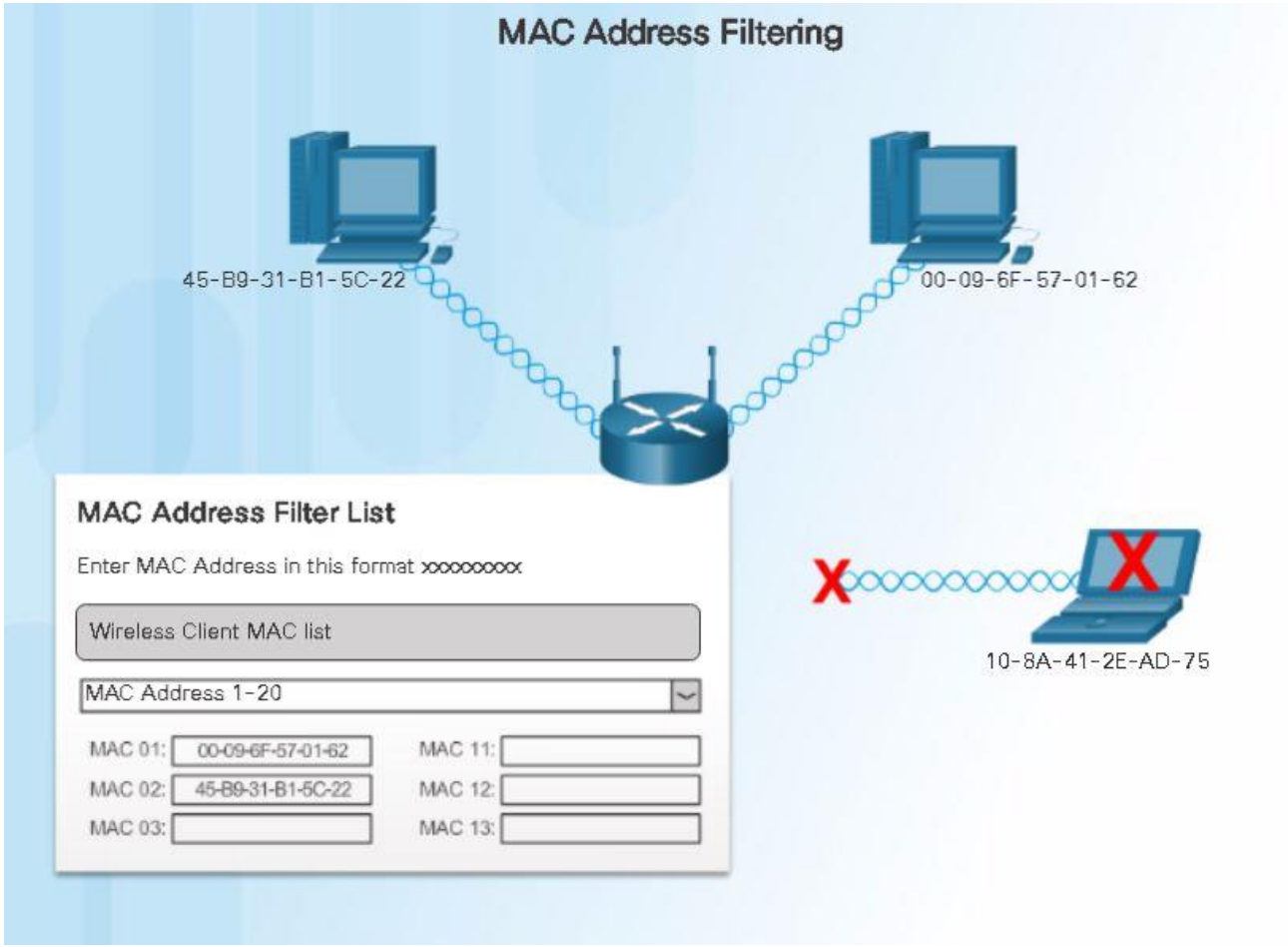
Фільтрація MAC-адрес

Один із способів обмежити доступ до приватної бездротової мережі полягає в тому, щоб точно контролювати, які пристрої можуть отримати доступ до такої мережі. Це може бути здійснено шляхом фільтрації MAC-адрес.

Фільтрація MAC-адрес використовує MAC-адресу, щоб визначити, які пристрої можуть підключатися до бездротової мережі. Коли бездротовий клієнт намагається підключити або зв'язатися з AP, він надсилатиме інформацію про MAC-адресу.

Якщо включена функція фільтрації MAC-адреси, бездротовий маршрутизатор або AP шукатимуть MAC-адресу з'єднання клієнта в попередньо сконфігурованій базі даних (рис. 4). Лише пристрої, MAC-адреси яких були записані в базі даних маршрутизатора, будуть дозволені для підключення.

Якщо MAC-адреса не наведена в базі даних, пристрою не дозволено з'єднуватися або спілкуватися в бездротовій мережі.



Є певні проблеми з таким видом безпеки. Наприклад, це вимагає, щоб MAC-адреси всіх пристроїв, які повинні мати доступ до мережі, були включені до бази даних, перш ніж з'являться спроби з'єднання. Пристрій, не ідентифікований у базі даних, не зможе підключитися. Крім того, пристрій зловмисника може клонувати MAC-адресу іншого пристрою, який має доступ.

Захист автентифікації користувачів

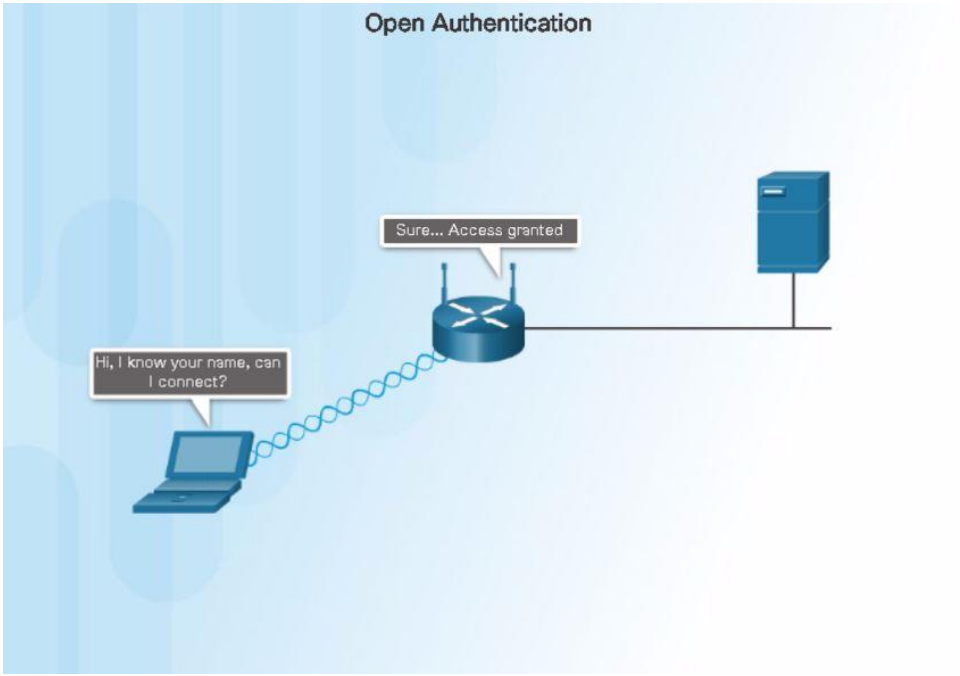
Окрім фільтрації MAC-адрес, інший спосіб контролювати, хто може підключитися до вашої мережі, - це здійснення автентифікації. Аутентифікація - це процес дозволу входу в мережу на основі набору верифікацій. Він використовується для перевірки того, що пристрою, який намагається підключитися до мережі, довіряють.

Використання імені користувача та пароля є найпоширенішою формою автентифікації. У бездротовому середовищі автентифікація все ще гарантує, що пов'язаний хост перевіряється, але обробляє процес підтвердження дещо іншим чином.

Аутентифікація, якщо вона ввімкнена, має з'явитися, перш ніж клієнт зможе підключитися до WLAN. Є три типи бездротових методів аутентифікації: відкрита аутентифікація, PSK та EAP.

Відкрита аутентифікація

За замовчуванням бездротові пристрої не вимагають автентифікації. Будь-який та всі клієнти можуть взаємодіяти незалежно від того, що вони є, як показано на рис. 5. Це називається відкритою автентифікацією.



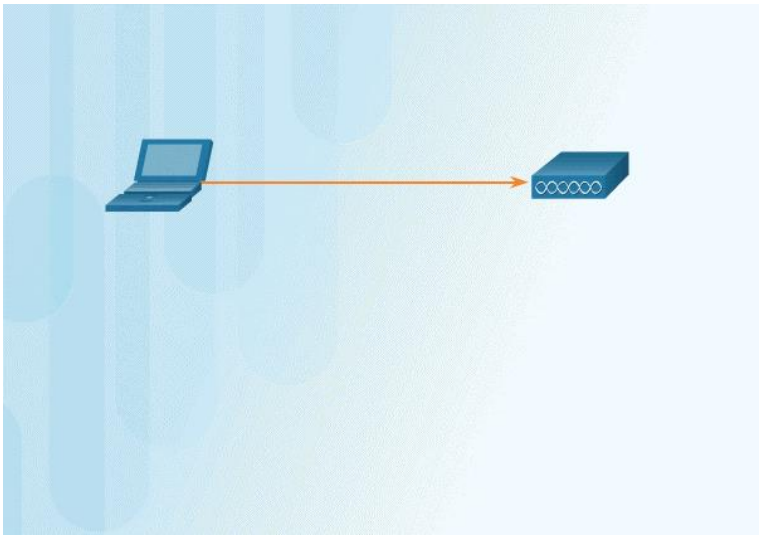
Відкрита автентифікація повинна застосовуватися лише у відкритих бездротових мережах, таких як ті, що знаходяться у школах та ресторанах. Він також може використовуватися в мережах, де автентифікація буде виконуватися іншими способами після підключення пристрою до мережі.

Утиліта налаштування для багатьох маршрутизаторів відключає відкриту автентифікацію та автоматично встановлює більш безпечну автентифікацію користувача в бездротовій приватній мережі.

Чи можу я увійти?

Після ввімкнення автентифікації, незалежно від використовуваного методу, клієнт повинен успішно пройти аутентифікацію, перш ніж він може зв'язуватися з AP і приєднатися до приватної мережі. Якщо ввімкнута і автентифікація, і фільтрація MAC-адрес, то перш за все відбувається автентифікація.

Коли аутентифікація буде успішною, AP перевірить MAC-адресу в таблиці MAC-адрес. При підтвердженні AP додає MAC-адресу хоста у свою таблицю хостів. Клієнт потім вважається пов'язаним з AP і може підключитися до мережі.

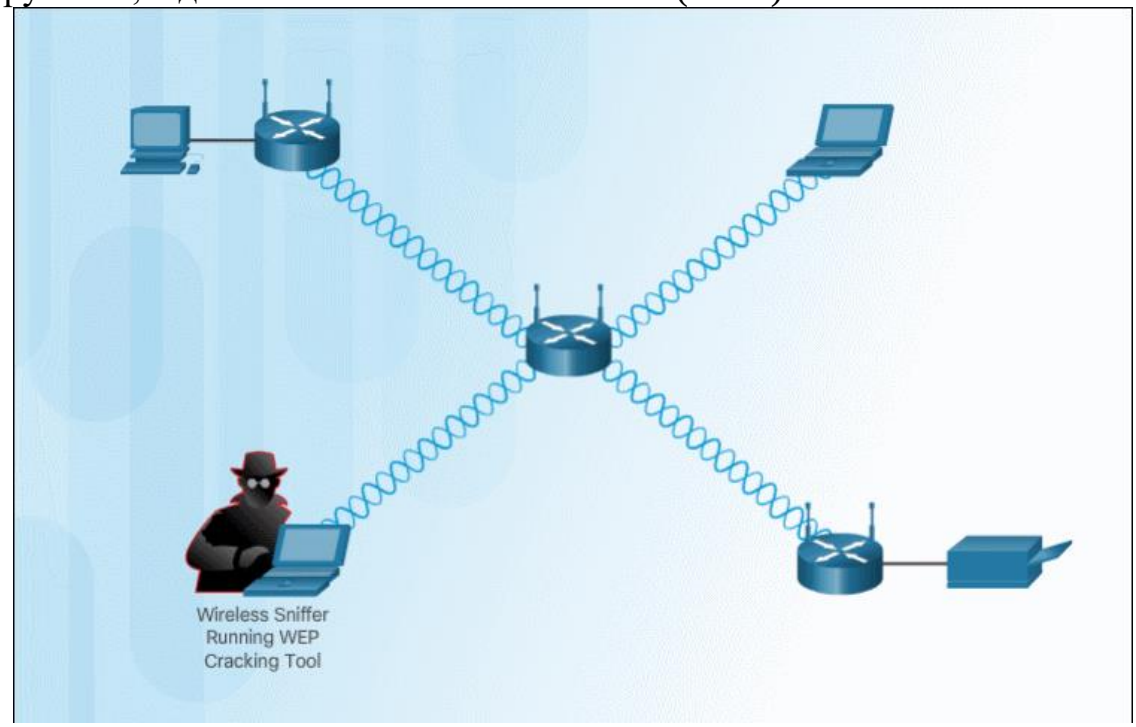


Технології шифрування для бездротових мереж

Ранні бездротові маршрутизатори використовували форму шифрування, відому як протокол Wired Equivalency Protocol (WEP) для забезпечення бездротових передач між клієнтами та точкою доступу. Протокол WEP - це функція захисту, яка шифрує мережевий трафік під час передачі по повітрю. WEP використовує попередньо налаштовані ключі для шифрування та дешифрування даних. Ключ WEP вводяться як рядок цифр і букв і, як правило, довжиною 64 біти або 128 біт. У деяких випадках WEP підтримує 256-бітні ключі шифрування.

Проте в WEP є слабкі сторони, включаючи використання статичного ключа на всіх пристроях з підтримкою WEP у бездротовій приватній мережі. Нападникам доступні програми, які можна використовувати для виявлення ключа WEP. Ці програми легко доступні в Інтернеті. Після того, як зловмисник витягнув ключ, він має повний доступ до всієї переданої інформації.

Один із способів подолання цієї уразливості - часто змінити ключ. Інший спосіб полягає у використанні більш просунутої та безпечної форми шифрування, відома як Wi-Fi Protected Access (WPA).



WPA2 також використовує ключі шифрування від 64 біт до 256 біт. Однак, WPA2, на відміну від WEP, створює нові динамічні ключі кожного разу, коли клієнт встановлює зв'язок з AP. З цієї причини WPA2 вважається більш безпечним, ніж WEP, оскільки його значно складніше зламати. Версія WPA2, призначена для домашніх мереж, позначається як WPA2-PSK. PSK вказує на те, що цей метод шифрування базується на попередньо розділеній клавіші, в даному випадку - за налаштуванням на парольну фразу користувача.

Важливо пам'ятати, що перед підключенням AP до мережі або Інтернет-провайдера слід запланувати та налаштувати заходи безпеки.

Деякі основні заходи безпеки, зокрема:

- змінити значення за замовчуванням для SSID, імен користувачів та паролів;

- відключити широкомовний SSID;
- налаштувати фільтрацію MAC-адрес.

Більш просунуті заходи безпеки включають:

- налаштування шифрування за допомогою WPA2;
- налаштування автентифікації;
- налаштування фільтрації трафіку.

Пам'ятайте, що жодна захисна міра поодинці не взмозі захистити бездротову мережу. Поєднання кількох методів посилить цілісність плану безпеки приватної мережі.

Під час налаштування клієнтів важливо, щоб ідентифікатор SSID відповідав SSID, налаштованому на AP. Ідентифікатори SSID чутливі до регістру, тому рядок символів має точно відповідати вимогам. Крім того, ключі шифрування та ключі автентифікації також повинні відповідати вимогам до їх створення.

Що хакери хочуть?

Чи проводові або бездротові, комп'ютерні мережі є важливими для повсякденної діяльності. Окремі люди та організації залежать від своїх комп'ютерів і мереж для таких функцій, як електронна пошта, облік, організація та керування файлами. Вторгнення неавторизованою людиною може призвести до відключень мережі та втрати роботи. Нападки на мережу можуть бути руйнівними і можуть призвести до втрати часу та грошей через пошкодження або крадіжку важливої інформації чи активів.

Зловмисники можуть отримати доступ до мережі через вразливість програмного забезпечення, апаратні атаки або навіть за допомогою менш високотехнологічних методів, таких як вгадування імені якогось користувача та пароля. Зловмисників, котрі отримують доступ шляхом модифікації програмного забезпечення або експлуатації вразливостей програмного забезпечення, часто називають хакерами.

Коли хакер отримує доступ до мережі, може виникнути чотири види загроз:

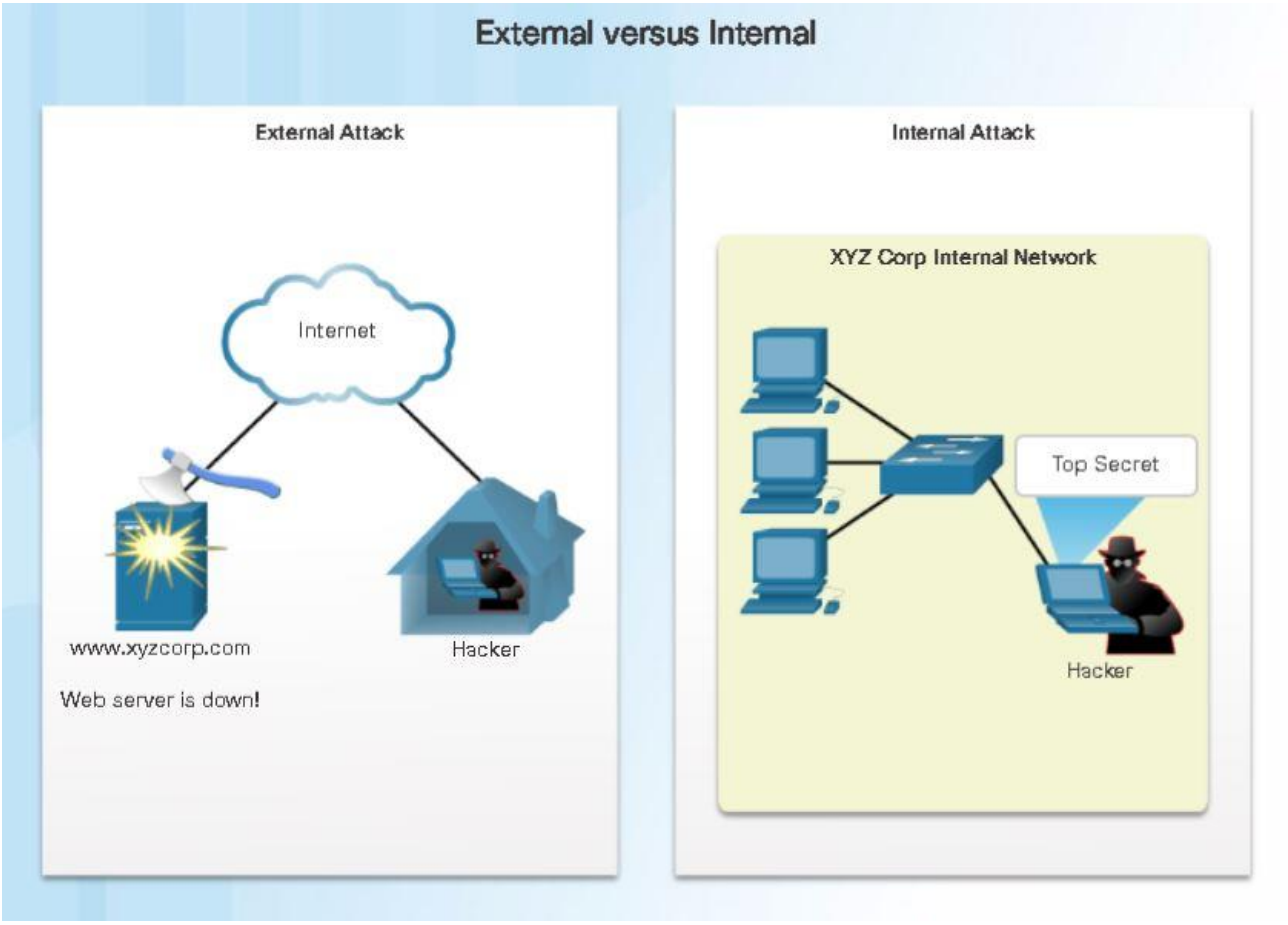
1) крадіжка інформації;
2) крадіжка особистих даних;
3) знищення даних/маніпуляції;
4) порушення обслуговування.

Звідки йдуть загрози безпеки?

Загроз безпеки від мережевих вторгнень може виникнути як з внутрішніх, так і ззовнішних джерел (рис. 8).

Зовнішні загрози

Зовнішні загрози виникають у людей, які працюють поза межами організації. Вони не мають авторизованого доступу до комп'ютерних систем чи мережі. Зовнішні зловмисники проникають в мережу в основному з Інтернету, бездротових каналів або серверів доступу до комутованого доступу.



Внутрішні загрози

Внутрішні загрози виникають, коли хтось уповноважує доступ до мережі через обліковий запис користувача або має фізичний доступ до мережевого обладнання. Внутрішній атакуючий знає внутрішню політику та людей. Вони часто знають, яка інформація є цінною і вразливою, та як дістатися до неї.

Проте не всі внутрішні напади є навмисними. У деяких випадках внутрішня загроза може виникнути від надійного працівника, який отримує (копіює) вірус або іншу загрозу безпеці, тоді за межами компанії він несвідомо вводить його в внутрішню мережу.

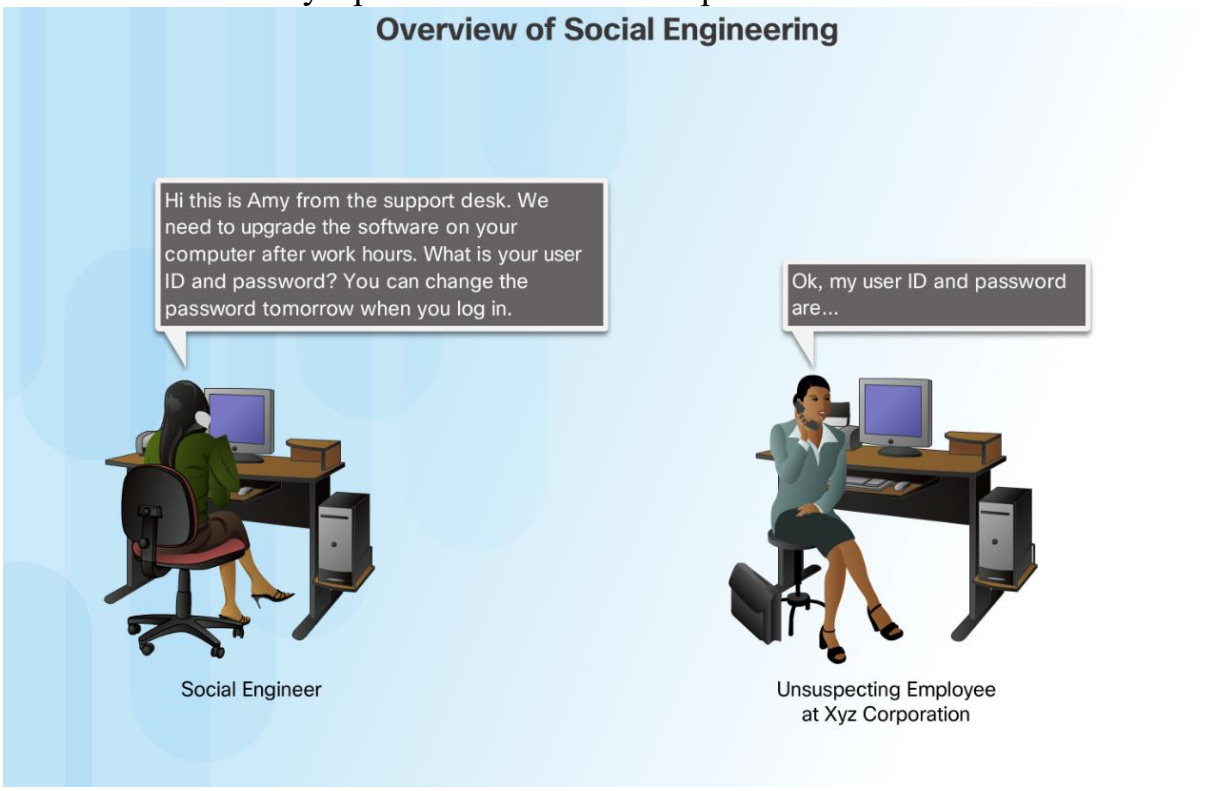
Один із найпростіших способів доступу до вторгнення, як внутрішнього, так і зовнішнього, – це використання людської поведінки. Одним з найбільш поширених методів експлуатації людських слабкостей називають соціальну інженерію.

Соціальна інженерія

Соціальна інженерія - це термін, який вказує на здатність щось чи когось впливати на поведінку людини чи групи людей. В контексті комп'ютерної та мережевої безпеки соціальна інженерія відноситься до набору методів, що використовуються для того, щоб обманути внутрішніх користувачів для виконання певних дій або виявлення конфіденційної інформації.

За допомогою цих методів атакуючий користується перевагами не підозрюваних законних користувачів, щоб отримати доступ до внутрішніх ресурсів та приватної інформації, таких як номери банківських рахунків або паролі (рис.9).

Соціальні інженерні атаки використовують той факт, що користувачі, як правило, вважаються одним з найслабших ланок в галузі безпеки. Соціальні інженери можуть бути внутрішніми або зовнішніми для організації, але найчастіше вони не зустрічаються з їхніми жертвами.



Використання довіри користувача

Три найбільш поширених способів, які хакери використовують для отримання інформації безпосередньо від авторизованих користувачів, це претекстинг, фішинг та вішінг.

Претекстинг

Претекстинг - це форма соціальної інженерії, де винайдений сценарій (привід чи претекст) використовується жертвою для того, щоб жертва розголосила інформацію або виконала дію. З цією метою, як правило, звертаються по телефону.

Для того, щоб претекстинг був ефективним, зловмисник повинен мати можливість встановити легітимні стосунки із запланованою метою або жертвою. Це часто вимагає певних попередніх знань або досліджень з боку атакуючого. Наприклад, якщо зловмисник знає номер соціальної страховки цілі, він може використовувати цю інформацію для отримання довіри. Тоді ціль більш схильна надати додаткову інформацію.

Фішинг

Фішинг - це форма соціальної інженерії, де фішер претендує на роль законної зовнішньої організації. Фішери, як правило, звертаються до цільової особи електронною поштою або текстовими повідомленнями. Фахівець може попросити перевірити інформацію, таку як паролі або імена користувачів, щоб запобігти надзвичайних наслідків.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102
2. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».
3. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)"
4. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. (ISO/IEC 27002:2013; Cor 1:2014, IDT).
5. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.
6. Методологія захисту інформації. Аспекти кібербезпеки: підручник / Г.М. Гулак – К.: Видавництво НА СБ України, 2020.
7. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
8. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
9. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення
10. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
11. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899
12. Стратегія національної безпеки України : Указ Президента України від 06.05.2015 р. № 287/2015// Офіційний вісник України. – 2015. – № 43. – С. 14. – Ст. 1353
13. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

Навчальне видання

ШТУЧНИЙ ІНТЕЛЕКТ ТА МАШИННЕ НАВЧАННЯ

Конспект лекцій

Укладачі: **Шебаніна** Олена В’ячеславівна
Тищенко Світлана Іванівна
Пархоменко Олександр Юрійович
Жебко Олександр Олегович
Коломієць Андрій Миколайович

Формат 60х84 1/16. Ум. друк. арк. 2.94.
Наклад 50 прим. Зам. № _____

Надруковано у видавничому відділі
Миколаївського національного аграрного університету
54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб’єкта видавничої справи ДК № 4490 від 20.02.2013