МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

АПАРАТНІ ТА ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання

Луцьк 2025

УДК 004.056(075.8)+681.518(075.8)
А76

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ І. С. Кондіус

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Н. П. Поліщук

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № 7 від 03 січня 2025 року.

Укладачі: _____ О. Л. Кайдик, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Т. В. Терлецький, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ С. М. Костючко, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: _____ Т. В. Терлецький, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

А76 **Апаратні та програмні засоби захисту інформації**: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 252 с.

У пропонованому виданні міститься тринадцять лекцій до курсу «Апаратні та програмні засоби захисту інформації».

Конспект лекцій ставить за мету сформувати у здобувачів освіти комплексне розуміння принципів, методів і технологій, які використовуються для захисту інформаційних систем. Лекційний матеріал акумулює у собі основну інформацію, яка є необхідною для отримання необхідних знань у сфері захисту інформації.

ВСТУП

У сучасному світі інформація є ключовим ресурсом, а розвиток засобів комунікації та нових інформаційних технологій є необхідною умовою формування глобального інформаційного суспільства. Такі технології покликані забезпечити можливість ефективного пошуку, оброблення, синтезу та передачі інформації з мінімальними матеріальними витратами. Інформаційні потоки, на сьогодні пронизали усі сфери суспільного життя, а уміння їх створювати та використовувати свідчить про успішність діяльності соціальних суб'єктів на будь-якому структурному рівні.

Однією із характерних рис інформаційного суспільства є зростання ролі інформації, яка стає не лише умовою ефективної діяльності, але й стратегічним ресурсом розвитку. Водночас, негативний вплив інформації може завдати серйозної шкоди. Такі загрози підкреслюють важливість сфери інформаційної безпеки, яка за сучасних умов набуває особливої актуальності та потребує нових досліджень для узагальнення існуючих даних, моделей та підходів, а також для створення інтегруючої основи, яка здатна протидіяти новим викликам.

Ознайомлення здобувачів освіти з курсом «Апаратні та програмні засоби захисту інформації» дозволить їм не лише отримати теоретичні знання, але й набути певних практичних навиків, які дозвлять, у майбутньому, ефективного реагування на виклики, що будуть поставати перед інформаційними системами.

Конспект лекцій об'єднує у собі необхідну інформацію, яку отримано із різноманітних першоджерел, та покликаний забезпечити ґрунтовну підготовку здобувачів першого (бакалаврського) рівня вищої освіти факультету комп'ютерних та інформаційних технологій освітньої програми «Інформаційні системи та технології охорони і безпеки».

ЗМІСТ

Сторінка

ЗМІСТОВНИЙ МОДУЛЬ 1. Основи методології захисту інформації

Тема 1. Основні поняття та структура інформаційної безпеки

План:

1.1 Теоретичні основи інформаційної безпеки

1.2 Принципи безпеки

1.1 Теоретичні основи інформаційної безпеки

Зауважимо, що словосполучення «інформаційна безпека» для різних контекстів може мати різне значення. Зазвичай, основна увага зосереджується на зберіганні, обробленні та передаванні інформації незалежно від того, якою мовою вона закодована, хто або що є її джерелом та який психологічний вплив вона чинить на людей.

Під інформаційною безпекою (ІБ) слід розуміти, перш за все, захищеність інформації інфраструктурою, яка її підтримує, від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин.

Захист інформації (ЗІ) – це комплекс заходів, які спрямовано на забезпечення інформаційної безпеки.

Як бачимо, правильний, із методологічної точки зору, підхід щодо проблем ІБ розпочинається із виявлення суб'єктів інформаційних відносин й інтересів цих суб'єктів, які пов'язані із використанням інформаційних систем (ІС). Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій.

Із вище викладеного можна зробити два важливих висновка.

1. Трактування проблем, які пов'язані із ІБ, для різних категорій суб'єктів може істотно відрізнятися (наприклад, порівнюємо режимні державні організації з навчальними інститутами: у першому випадку «нехай краще усе зламається, ніж ворог довідається хоча б один секретний біт», у другому – «немає у нас ніяких секретів, аби тільки все працювало»).

2. Інформаційна безпека не зводиться лише до захисту інформації від несанкціонованого доступу (НД), це є принципово більш широке поняття. При цьому суб'єкт інформаційних відносин може постраждати (зазнати збитків) не лише від несанкціонованого доступу, але й від поломки системи, яка викликала перерву в роботі (для багатьох відкритих організацій саме захист інформації від НД, за важливістю, перебуває аж ніяк не на першому місці).

Термін «комп'ютерна безпека» прийнято вважати еквівалентом ІБ. При цьому комп'ютери є однією із складових ІС, основна увага якої зосереджується на інформації, яка зберігається, оброблюється та передається за їх допомогою, а безпека визначається усією сукупністю її складових.

Відповідно до визначення ІБ вона залежить не лише від комп'ютерів, але й від інфраструктури, яка її підтримує (системи електро-, водо- та теплопостачання, кондиціонування, комунікативні засоби й обслуговування). Слід пам'ятати, що будь-яка інфраструктура має свою, самостійну, цінність, відповідно, основна увага повинна зосереджуватись на тому як вона впливає на виконання ІС закладених у неї функцій.

Проаналізувавши термін «інформаційна безпека» перед іменником «збиток» стоїть прикметник «неприйнятний». Отже, застрахуватися від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільно, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Тому, із чимось доводиться миритися й захищатися необхідно тільки від того, з чим змиритися ніяк не можна.

Як бачимо основною метою ЗІ є зменшення розмірів збитків до припустимих значень. При цьому захист інформації стає важливою складовою частиною підтримання національної безпеки.

Організація ЗІ здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Реалізація організаційних та інженерно-технічних заходів становлять суть процесів технічного захисту інформації (ТЗІ). Правові заходи захисту інформації є базисом, на який спираються організаційні та інженерно-технічні заходи захисту інформації.

Одним із визначень терміну «інформація» є зафіксоване на будь-якому носії уявлення про предмети, процеси, події, явища тощо. При цьому під терміном «фіксація» необхідно розуміти закріплення будь-чого у певному положенні або вигляді (наприклад, письмове закріплення відомостей, думки тощо). Інформація, для свого функціонування, постійно вимагає наявності носія. Водночас, носієм інформації може бути поле або речовина (у деяких випадках – людина). Під час інформаційних відносин, в залежності від напрямку переміщення інформації, носії інформації прийнято поділяти на носії-джерела та носії-отримувачі.

В Законі України «Про інформацію» під джерелом інформації прийнято розуміти документи або інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію. Щодо отримувачів, то вони сприймають інформацію через той або інший сенсор (давач чи вимірювальний перетворювач). При цьому процеси її сприйняття та перетворення можуть бути досить складними.

Сприйняття інформації включає у себе наступні етапи:

– виявлення об'єкта у полі сприйняття;

– розрізнення окремих ознак всередині об'єкта;

– виділення в об'єкті інформативного змісту, який буде адекватним меті дії;

– формування образу сприйняття.

В терміні «інформація», під уявленням необхідно розуміти образ та/або суть предмету, процесу, події, природного явища тощо, які сприймаються сенсорами приладів або, безпосередньо, органами чуття, а також створені відтворювальною і/або творчою уявою людини чи елементами штучного інтелекту різних пристроїв.

Водночас уява – це психічна діяльність людини, яка полягає у створенні уявлень та уявних ситуацій, яка, в цілому, не сприймалася нею в реальній дійсності (творча уява) або відтворення колишніх вражень і спогадів, які спираються на її життєвий досвід (відтворювальна уява). Хоча, відтворювальна й творча уява, зазвичай, розрізняються на аналітичному рівні, ці компоненти тісно взаємодіють між собою під час формування уявлень. На практиці, прийнято вважати, що інформація володіє деякими істотними, з огляду на її захист, властивостями. При цьому, такі властивості, з точки зору як користувача, так і власника інформації, можна розглядати у форматі деяких бажаних станів інформації (носіїв інформації).

Основні властивості інформації:

– конфіденційність (властивість інформації бути захищеною від несанкціонованого ознайомлення);

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

– доступність (властивість інформації бути захищеною від несанкціонованого блокування).

Відповідно до вищеперерахованих властивостей, ТЗІ – це діяльність, яка спрямована на забезпечення організаційними та інженерно-технічними заходами конфіденційності, цілісності й доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту. Події, які можуть, потенційно, порушити одну із названих властивостей інформації прийнято називати загрозами порушення конфіденційності, цілісності та доступності інформації. Закон України «Про інформацію» класифікує усю інформацію за режимом доступу, тобто передбаченого певними правовими нормами порядку її отримання, використання, поширення та зберігання (рис. 1.1).

Рисунок 1.1 – Законодавча класифікація видів інформації в Україні

До секретної (особливої важливості – ОВ; цілком таємної – ЦТ та таємної – Т) належить інформація, яка містить відомості, що становлять державну або іншу передбачену Законом таємницю, розголошення якої завдає шкоди суспільству/державі.

До конфіденційної інформації належать відомості, якими володіють, які використовують або якими розпоряджаються окремі фізичні або юридичні особи, котрі поширюють їх відповідно до визначених ними самостійно умов.

Секретна та конфіденційна інформація потребує захисту від загроз порушення конфіденційності, цілісності та доступності, а відкрита інформація важлива для осіб, суспільства та держави – захисту від загроз порушення цілісності й доступності.

Враховуючи визначення інформації та суть ТЗІ прийнято формувати парадигму захисту інформації: інформація вважається захищеною, якщо під час її переміщення дотримуються режимної адекватності комунікаційних носіїв інформації. Як бачимо, порушення інформаційної безпеки можливе лише за умови переміщення інформації.

Формулювання парадигм потребує формування визначень, які мають сприйматися усіма учасниками процесу однаково. Отже, під час переміщення інформації необхідно розуміти зміну просторових координат носіїв з інформації або знищення інформації із збереженням або руйнуванням носія. У ході переміщення інформації можливою є зміна її носія.

Поняття «режимна адекватність» формується із двох термінів «режим» і «адекватність». Режим – це сукупність норм, які використовуються для досягнення будь-якої мети (обов'язково враховують режим доступу до

інформації, який передбачено правовими нормами). Адекватність – це відповідність, правильність, точність. Термін «комунікаційний» прийнято застосовувати для суміщення (здатність до спільної роботи) різнотипних систем передачі інформації.

Комунікаційні носії інформації – це носії інформації, здатні до взаємодії (наприклад, некомунікаційними носіями є органи зору, у людини, які не здатні сприйняти голосову (акустичну) інформацію, а комунікаційним носієм, орган зору, виступає під час сприйняти інформацію, яка зафіксована на паперовому носії зрозумілою для нього мовою).

Смислове значення складових терміну «режимна адекватність носіїв інформації» полягає у відповідності режимів доступу носіїв інформації (джерела й отримувача) під час їх взаємодії (наприклад, режимна неадекватність – ознайомлення із змістом секретного документа без права на доступ до секретної інформації, а режимна адекватність – особиста розмова двох осіб, які здатні передати або отримати інформацію із обмеженим доступом, що є власністю одного з них). Проміжні носії інформації, так само, як і носій-джерело або носій-отримувач, повинні відповідати вимогам режимної адекватності та комунікаційності.

Іншими словами, режимна адекватність комунікаційних носіїв інформації – це їх здатність брати участь в інформаційному обміні під час відповідності режимів доступу. Сформульована вище парадигма враховує основні інформаційні загрози таким чином: загрози конфіденційності спрямовано на заборонене режимом доступу переміщення інформації від носія-джерела до носія-отримувача. При цьому, інформація зберігає конфіденційність, за умови якщо дотримується, насамперед, режимна адекватність носіїв інформації.

Загрози цілісності інформації направлені на заборонену режимом доступу (порядком отримання, використання, поширення та зберігання інформації) зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно або внаслідок об’єктивного впливу навколишнього середовища, яке оточує носій інформації. Інформація зберігає цілісність, за умови коли дотримується встановлена режимна адекватність відносно правил її модифікації (видалення). Будь-який суб’єкт, який впливає на носій джерела інформації, з метою модифікації інформації, необхідно розглядати у якості носія інформації, який несе у собі уяву про необхідну модифікацію (видалення) інформації носія джерела інформації.

Під час модифікації відбувається й переміщення інформації, яка модифікується. Вплив об’єктів, процесів зовнішнього середовища та інших

чинників, які часто відносять до розряду «випадкових» – це невідповідність джерела-носія інформації встановленому режиму доступу, що часто призводить до порушення комунікаційності. Цей вплив прийнято вважати порушенням режимної адекватності, і як наслідок – комунікаційності носіїв інформації. Загрози доступності (відмова в обслуговуванні) спрямовані на навмисне або ненавмисне порушення комунікаційності носіїв інформації під час їх взаємодії. Порушення комунікаційності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, за умови коли зберігається комунікаційність носіїв інформації під час їх взаємодії.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією. Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України, та які визначено у порядку, який встановлено Законом України «Про державну таємницю», державною таємницею і підлягають захисту державою. Матеріальні носії секретної інформації – матеріальні об'єкти, зокрема фізичні поля, в яких відомості, які становлять державну таємницю, відображено у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, які використовують необхідні засоби та методи захисту інформації, яка становлять державну таємницю та їх носіїв, а також заходів, що проводяться із цією метою.

Гриф секретності – це реквізит матеріального носія секретної інформації, який засвідчує ступінь секретності цієї інформації.

Комерційна таємниця – відомості, які не є державною таємницею, та пов'язані із виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати збитку їх інтересам.

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

Переліки конфіденційної інформації, яка є власністю держави і якій надається гриф обмеження доступу «Для службового користування», розробляють і вводять в дію міністерствами, іншими центральними органами виконавчої влади, обласними, міськими державними адміністраціями.

1.2 Принципи безпеки

Варто пам'ятати, що принципи забезпечення інформаційної безпеки повинні містити перш за все: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграцію з міжнародними системами безпеки; економічну ефективність.

Варто розуміти, що, на практиці, неможливо створити таку систему, захист якої не можна буде зламати, а основним принципом виступає створення такого механізму захисту, вартість злому якого буде дорожчим за інформацію, яку можна отримати. Зважаючи на це, необхідним є впровадження програмних засобів безпеки, які входять до складу програмного забезпечення системи та є необхідними для виконання функцій захисту. Не варто забувати і про те, що усунення наслідків кібератак часто обходиться у декілька разів дорожче за профілактику боротьби з ними. В сучасних реаліях сьогодення забезпечення належного захисту інформації напряму пов'язане із забезпеченням стабільного економічного розвитку як окремого підприємства, так і держави в цілому.

Розвиток ТЗІ в Україні обумовлюється наступними чинниками:

– стрімким розвитком суспільних і міждержавних відносин;

– застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва;

– поширенням засобів несанкціонованого доступу до інформації.

Нормативними документами у сфері ТЗІ визначено такі основні загрози безпеці інформації в Україні:

– діяльність інших держав, яка спрямована на отримання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

– недосконаліть організації в Україні міжнародних виставок засобів різноманітного призначення (особливо пересувних) і заходів екологічного моніторингу, які можуть використовуватися для отримання інформації, яка носить розвідувальний характер;

– діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямована на отримання переваги у політичній боротьбі та конкуренції;

– злочинна діяльність, спрямована на протизаконне отримання інформації з метою досягнення матеріальної вигоди або заподіяння шкоди юридичним або фізичним особам;

– недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також низька кваліфікація технічного персоналу;

– використання інформаційних технологій низького рівня, які призводять

до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ.

Варто відзначити, що з метою протидії існуючим інформаційним загрозам в Україні триває процес створення системи ТЗІ. Система ТЗІ являє собою сукупність суб'єктів, які об'єднані одними і тими ж цілями й завданнями захисту інформації, організаційними та інженерно-технічними заходами, нормативно-правовою та матеріальною базою.

Державна політика у сфері ТЗІ формується та реалізується із урахуванням наступних принципів:

– дотримання балансу інтересів особи, суспільства й держави, їх взаємної відповідальності;

– єдності підходів до забезпечення ТЗІ, які зумовлені загрозами безпеці інформації та режимом доступу до неї;

– комплексності, повноти й безперервності заходів ТЗІ;

– відкритості нормативно-правових актів й нормативних документів із питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

– узгодженості нормативно-правових актів й нормативних документів із питань ТЗІ з відповідними міжнародними договорами України;

– обов'язковості захисту інженерно-технічними заходами: інформації, що становить державну та іншу передбачену законом таємницю;

– конфіденційної інформації, що є власністю держави;

– відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює;

– відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, на підприємствах, в установах та організаціях;

– виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту;

– ієрархічність побудови організаційної структури системи ТЗІ та керування її діяльністю в межах повноважень, визначених нормативно-правовими актами;

– методичне керування спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

– координація дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки.

До 01.01.2007 року спеціально уповноваженим центральним органом

виконавчої влади, на який було покладено відповідальність за формування та реалізацію державної політики у сфері ТЗІ, був Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України. З 01.01.2007 року, на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації й відповідних підрозділів СБУ, відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» створено Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язок).

У якості суб'єктів у системі ТЗІ України виступають:

– Держспецзв'язок;

– органи, відносно яких здійснюється ТЗІ;

– державні наукові, науково-дослідні та науково-виробничі підприємства, установи та організації, які належать до системи СБУ і виконують завдання технічного захисту інформації;

– військові частини, підприємства, установи та організації усіх форм власності та громадяни-підприємці, які здійснюють діяльність відносно ТЗІ за відповідними дозволами або ліцензіями;

– навчальні заклади з підготовки, перепідготовки й підвищення кваліфікації фахівців із технічного захисту інформації.

Усі заходи, які пов'язані із захистом інформації, яка є власністю держави, координуються й контролюються Держспецзв'язком. Основні завдання усіх суб'єктів системи ТЗІ України зазначаються у відповідних нормативних документах. При цьому, конкретним об'єктом захисту, зазвичай виступає не розрізнений носій інформації, а об'єднані загальними завданнями його впорядкована сукупність. Враховуючи це, під об'єктом захисту слід розуміти інформаційну систему, яка реалізує автоматизоване збирання й оброблення даних формується із технічних та допоміжних засобів, програмного забезпечення й відповідного персоналу (рис. 1.2).

Зазвичай систему захисту інформації (СЗІ), для конкретних об'єктів (інформаційних систем), доцільно подавати у вигляді:

– основ побудови системи захисту інформації;

– напрямів захисту інформації;

– етапів побудови СЗІ.

Основа побудови системи захисту інформації.

1. Законодавча, нормативно-правова, наукова і методична бази забезпечення захисту інформації.

Структура й завдання органів (підрозділів), що забезпечують безпеку

інформаційних технологій.

3. Організаційно-технічні та режимні заходи і методи захисту інформації.

4. Програмно-технічні методи й засоби, використовувані для захисту інформації.

Рисунок 1.2 – Складові інформаційної системи

Напрямки захисту інформації прийнято визначати із урахуванням конкретних особливостей ІС, як об'єкта захисту. Найбільш поширеними, із врахуванням типової структури ІС та видів робіт із ІЗ, прийнято вважати наступні напрямки:

– захист об'єктів інформаційних систем;
– захист процесів, процедур і програм оброблення інформації;
– захист каналів зв'язку;
– блокування побічних електромагнітних випромінювань та наводок;
– керування системою захисту.

Етапи побудови СЗІ проводяться однаково, для усіх та кожного окремо напрямів. Наявний практичний досвід дозволяє виділити такі етапи побудови системи захисту інформації:

– визначення інформаційних ресурсів (ІР), які потребують захисту;
– виявлення повної множини загроз безпеці ІР, які потребують захисту;
– проведення оцінювання вразливості та ризиків для ІР, які потребують захисту, відповідно до виявленої множини загроз;
– розроблення проєкту/плану системи ЗІ, яка знижує за вибраним критерієм ризики для ІР, що потребують захисту, відповідно до виявленої множини загроз;
– реалізація проєкту/плану захисту інформації;
– визначення якості реалізованої системи захисту;
– здійснення контролю функціонування та керування системою захисту.

За можливістю, проходження етапів здійснюється безперервно у замкненому циклі, із проведенням відповідного аналізу стану СЗІ та уточненням вимог до неї після кожного кроку.

Для опису логічних зв'язків та більш детального подання процесу захисту інформації для кожної ІС необхідно сформувати матрицю знань інформаційної

безпеки. Так матриця об'єднує логічно складові блоків «основи», «напрями» і «етапи» за принципом кожен із кожним. Варто пам'ятати, що матриця формується із врахуванням конкретних завдань по створенню відповідної СЗІ для конкретної ІС.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою інформаційна безпека та захист інформації?
2. Технічний захист інформації та його суб'єкти.
3. Інформація та етапи її сприйняття.
4. Класифікація інформації та її властивості.
5. Комунікаційні носії інформації.
6. Об'єкти захисту та загрози доступності.
7. Протидія інформаційним загрозам.
8. Державна політика у сфері ТЗІ.
9. Система захисту інформації та напрямки захисту інформації.
10. Етапи побудови СЗІ.

Рекомендована література: [1-17].

Тема 2. Концептуальні засади забезпечення інформаційної безпеки в Україні

План:

2.1 Інформаційна безпека як складова національної безпеки

2.2 Нормативно-правове забезпечення інформаційної безпеки

2.1 Інформаційна безпека як складова національної безпеки

На сьогодні інформаційні системи та інформаційно-телекомунікаційні мережі підтримують сервіси та передають дані у таких об'ємах, які було тяжко собі уявити ще декілька років тому. Їх готовність необхідна, насамперед, для роботи різноманітних інфраструктур (комунальні або електричні мережі, органи державного, муніципального та регіонального управління, організації, населення тощо), а безпека цих систем стає необхідною умовою їх подальшого розвитку. Тому кожному випадку інформаційної безпеки притаманна своя специфікація політики безпеки, тобто множина бажаних цілей (електронній системі голосування притаманна така ознака, коли голосує тільки зареєстрована у ній особа; доступ до сервера надається тільки автентифікованому користувачу; до банківської системи підключається лише авторизований користувач, тощо).

Безпека об'єкта виражається через безпеку його найбільш важливих властивостей або властивостей структурних складових. Якщо об'єктом безпеки виступає людина, то її безпека полягає у захищеності живого організму на рівні психічних і духовних властивостей особистості. У тому випадку коли об'єктом безпеки є суспільство – у захищеності від загроз усіх його членів та історичних відносин між ними.

Щодо національної безпеки, то її слід розрізняти: державна, економічна, суспільна, оборонна, інформаційна, екологічна та інші види безпеки.

Безпека являє собою протидію, на заданому рівні, спробам нанести шкоду функціонуванню об'єкту захисту в цілому, або його структурним складовим.

Однією із найважливіших структурних складових багатьох об'єктів безпеки є інформація або пов'язана дотично діяльність, предметом якої виступає інформація.

Варто зауважити, що зараз широкого поширення набуло поняття інформаційної безпеки, яке підкреслює важливість інформації в сучасному суспільстві та характеризує той факт, що інформаційний ресурс на сьогодні є таким же багатством, як корисні копалини, виробничі й людські ресурси, і так само як і вони підлягає захисту від різного роду посягань, зловживань і злочинів.

Під інформаційною безпекою прийнято розуміти захищеність інформації та підтримуючої її інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які супроводжуються нанесенням різного ступеню шкоди їх власникам або користувачам.

Різноманітність підходів до вирішення проблем, які дозволять забезпечити стійкість інформаційної безпеки, здійснюють на етапі виявлення суб'єктів, які зацікавлені у забезпеченні:

– своєчасного доступу до необхідної інформації;

– конфіденційність певної частини інформації;

– достовірність (повнота, точність, адекватність, цілісність) інформації;

– захисту від нав'язування неправдивої (недостовірної, перекрученої) інформації (дезінформації);

– захисту частини інформації від незаконного тиражування (захисту авторських прав, прав власника інформації тощо);

– можливості здійснення безперервного контролю і управління процесами обробки та передачі інформації;

– розмежування відповідальності за порушення законних прав (інтересів) інших суб'єктів інформаційних відносин та встановлених правил поводження з інформацією.

Забезпечення наведених вимог є суттєвим важелем захисту інформаційної безпеки як для держави в цілому, так і для окремих громадських (комерційних) організацій, підприємств (юридичних осіб) та окремих громадян (фізичних осіб), які виступають суб'єктами інформаційних відносин.

Суб'єкт – це активний компонент інформаційної системи, який може стати причиною витоку інформації від об'єкта до суб'єкта або зміни стану системи.

Об'єкт – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту формує доступ до інформації, яка міститься у ньому.

У якості об'єктів, які підлягають захисту в інтересах забезпечення безпеки суб'єктів інформаційних відносин, зазвичай розглядають: інформацію та інформаційні ресурси, носії інформації, процеси оброблення інформації.

Під інформацією слід розуміти відомості про об'єкти та явища навколишнього середовища, їх параметри, властивості та стан, які дозволять зменшити ступінь зовнішнього впливу.

До основних властивостей якості інформації з точки зору користувача варто віднести: презентативність, змістовність, достатність, доступність, актуальність, своєчасність, точність, достовірність та сталість.

Інформаційні ресурси – це окремі документи та масиви документів, які можуть бути представлені самостійно або у вигляді інформаційної системи. На практиці їх прийнято класифікувати:

– за видом інформації: правові, науково-технічні, політичні, фінансово-економічні, статистичні, метрологічні, соціальні, персональні, медичні тощо;

– за режимом доступу: відкриті, обмеженого доступу, державна таємниця, конфіденційна інформація, комерційна таємниця, професійна таємниця, службова таємниця, особиста (персональна) таємниця;

– за формою власності: державні, муніципальні, регіональні, приватні, колективні;

– за видом носія: на папері (документи, листи, медичні карти, телефонні довідники організацій, чернетки тощо), на екрані, в пам'яті ПК, у каналі зв'язку, на гнучких і жорстких магнітних дисках, на інших носіях.

Носіями інформації можуть виступати й окремі люди, які володіють важливою інформацією (експерти), а також спеціально завербовані або випадкові інформатори.

Поінформованість кінцевого користувача про заходи безпеки повинна проявлятися в умінні розрізняти 4 рівні захисту комп'ютерних та інформаційних ресурсів:

– запобігання (доступ до інформації та технологій має тільки авторизований персонал);

– виявлення (про зловживання стає відомо ще на ранній стадії, навіть під час обходу механізмів захисту);

– обмеження (зменшення розміру втрат, у випадку коли злочин мав місце, незважаючи на вжиті заходи щодо його запобігання);

– відновлення (забезпечення ефективного відновлення інформації при наявності документованих і перевірених планів проведення цієї операції).

Під безпекою комп'ютерних систем прийнято розуміти її захищеність від випадкового або навмисного втручання у нормальний процес її функціонування, а також від спроб розкрадання, зміни або руйнування її компонентів.

Щодо природи впливів на КС, то вона може бути найрізноманітнішою – стихійні лиха (землетруси, урагани, пожежі), вихід з ладу її складових елементів, помилки персоналу, спроба проникнення зловмисника.

Безпека КС досягається шляхом застосування заходів забезпечення конфіденційності та цілісності оброблюваної нею інформації, а також доступності й цілісності компонентів і ресурсів системи.

Під доступом до інформації варто розуміти ознайомлення з інформацією, її оброблення, зокрема копіювання, модифікація або знищення інформації. На практиці розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації – це доступ до інформації, що не порушує встановлені правила розмежування доступу. Ці правила призначені для регламентування права суб'єктів на доступ до об'єктів.

Несанкціонований доступ до інформації характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп'ютерних порушень.

Конфіденційність даних – це статус, наданий даними і визначає необхідний ступінь їх захисту. За суттю конфіденційність інформації – це властивість інформації бути відомою тільки допущеним особам (авторизованим суб'єктам системи). Для інших суб'єктів системи ця інформація повинна бути невідомою.

Цілісність інформації забезпечується у тому випадку, коли дані в системі не відрізняються в семантичному відношенні відносно даних у вихідних документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування.

Цілісність компонента або ресурсу системи – це властивість компонента або ресурсу бути незмінним в семантичному сенсі під час функціонуванні системи в умовах випадкових або навмисних спотворень (руйнівних впливів).

Доступність компонента або ресурсу системи – це властивість компонента або ресурсу бути доступним для авторизованих законних суб'єктів системи.

Метою захисту систем обробки інформації є протидія загрозам безпеки. Під загрозою безпеки КС прийнято розуміти можливі дії, які прямо або побічно можуть завдати шкоди її безпеки.

Комплекс засобів захисту являє собою сукупність програмних і технічних інструментів, що створюються і підтримуються для забезпечення інформаційної безпеки КС. Такий комплекс створюють і підтримують відповідно до прийнятої в організації політики безпеки.

Політика безпеки – це сукупність норм, правил і практичних рекомендацій для надійної роботи засобів захисту КС від безлічі загроз. До найважливіших аспектів ІБ відносять: доступність, цілісність і конфіденційність.

Розглянемо основні поняття, категорії, визначення та терміни.

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

2. Єдиний інформаційний простір країни – це сукупність інформаційних ресурсів та інформаційної інфраструктури, що дозволяє на основі єдиних принципів і за загальними правилами забезпечувати безпечну інформаційну взаємодію держави, організацій й громадян за їх рівнодоступністю до відкритих інформаційних ресурсів, а також, максимально повне задоволення їх інформаційних потреб на усій території країни при збереженні балансу інтересів на входження до світового інформаційного простору та забезпечення національного інформаційного суверенітету.

3. Інформаційні ресурси – інформаційна інфраструктура (апаратура й системи створення, обробки, збереження і передачі інформації), включаючи файли та бази даних, інформацію й інформаційні потоки.

4. Загроза інформаційній безпеці – це такий стан, коли проявляються наміри або дії, які можуть нанести шкоду інтересам особистості, суспільства та держави в галузі інформації.

5. Незаконне використання інформаційних та телекомунікаційних систем й інформаційних ресурсів – їх використання без відповідного дозволу або порушення встановлених правил, законодавства чи принципів міжнародного права.

6. Інформаційна інфраструктура включає у себе:

– організаційні структури, які забезпечують функціонування та розвиток єдиного інформаційного простору (при цьому, забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове, фінансове забезпечення);

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

– телекомунікаційні технології;

– системи засобів масової інформації.

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

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

На сучасному етапі розвитку суспільства основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері прийнято вважати:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну або іншу таємницю, а також конфіденційної інформації, яка є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

2.2 Нормативно-правове забезпечення інформаційної безпеки

Базові засади інформаційної безпеки України закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України.

Закон України «Про інформацію» закріплює право громадян України на інформацію та встановлює правові основи інформаційної діяльності. Закон стверджує інформаційний суверенітет України і визначає правові форми

міжнародного співробітництва в галузі інформації, встановлює загальні правові основи отримання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

При цьому, інформація визначається як документовані або публічно оголошені відомості про події та явища, які відбуваються у суспільстві, державі та навколишньому природному середовищі. Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Усі громадяни України, юридичні особи і державні органи мають право на інформацію, яка передбачає можливість вільного отримання, використання, поширення та зберігання відомостей, які необхідні для них, з метою подальшої реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Слід пам'ятати, що для кожного громадянина забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

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

Відповідно до чинного законодавства України поняття «інформаційна безпека» – стан захищеності життєво-важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

На практиці виділяють три рівня забезпечення інформаційної безпеки:

– рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору);

– суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);

– державний рівень (інформаційно-аналітичне забезпечення діяльності

державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

Концепція державної інформаційної політики. Досі не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Протягом 2002-2010 років було три спроби ухвалити концепцію державної інформаційної політики в 2002, 2009 та 2010 роках. У січні 2011 року черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради України з питань свободи слова та інформації.

Однією з основних загроз інформаційній безпеці Закону України «Про основи національної безпеки» називає «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації».

До інших загроз віднесено: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

В Доктрині інформаційної безпеки України, яка була підписана у 2009 році, виділено наступні загрози інформаційній безпеці країни:

– поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

– зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

– деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України;

– прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками.

Слід зазначити, що після подій на Євромайдані у 2014 році розпочалась розробка нової Доктрини інформаційної безпеки, яка відповідає новим вимогам сьогодення.

Діяльність Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки. При Раді національної безпеки і оборони (РНБО) діє Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки. До основних її завдань належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики.

Закони України:

– Закон України «Про інформацію» від 02.10.1992 № 2657-XII;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР;

– Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;

– Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.

Постанови КМУ:

– Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373;

– Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893.

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування комп'ютерних систем захисту інформації:

– ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі;

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу;

– НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2;

– НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу;

– НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

– НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Галузеві стандарти:

– ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD);

– ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD).

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою інформаційна сфера та інформаційні ресурси?
2. Що являє собою єдиний інформаційний простір країни?
3. Що являє собою загроза інформаційній безпеці?
4. Які складові включає у себе інформаційна інфраструктура?
5. Які базові засади ІБ закладено в Конституції України?
6. Які види інформації визначаються Законом України «Про інформацію»?
7. Як поділяється інформація за режимом доступу до неї?
8. Яка інформація входить до інформаційних ресурсів України?
9. Технічний захист інформації та правова основа його забезпечення.
10. Чим зумовлені загрози безпеці інформації в Україні?
11. Які принципи формування та проведення державної політики у сфері технічного захисту інформації?
12. Основні напрями державної політики у сфері ТЗІ?

Рекомендована література: [1-17].

Тема 3. Методи та засоби захисту в інформаційній безпеці. Огляд безпеки системи

План:

3.1 Захист інформації та його основні завдання

3.2 Методи проведення атак на інформацію

3.3 Класифікація методів і засобів захисту інформації

3.4 Інформація з обмеженим доступом

3.5 Структура політики безпеки та її основні частини

3.6 Життєвий цикл розробки систем безпеки

3.1 Захист інформації та його основні завдання

На сьогоднішній день переважна більшість інформації має бути захищеною. Принципи її захисту повинні бути різними, та залежать від того, який тип інформації необхідно захищати. У тому випадку коли інформація відповідає одному із класифікованих ступенів секретності, то до системи захисту висувають лише ті умови, які зосереджено на захисті її конфіденційності.

На практиці, до відкритої інформації прийнято висувати свої вимоги щодо захищеності, оскільки захищеними мають бути як її цілісність, так і доступність.

Діяльність, яка спрямована на забезпечення захисту конфіденційності, цілісності та доступності важливої для держави, суспільства та особи інформації, в тому числі відкритої, захист якої передбачено законом, прийнято називати захистом інформації.

У даний час, фахівці цієї галузі оперують багатьма поняттями, які дозволяють визначити ступінь захисту інформації в системах обробки та передавання інформації. Сюди ж відносять: захист інформації в комп'ютерних системах, захист інформації в автоматизованих системах, захист інформації в інформаційно-телекомунікаційних мережах тощо. Причому прийнято вважати, що усі ці поняття є синонімами, хоча насправді це не зовсім так.

Враховуючи те, що за останні роки термінологія у сфері захисту інформації зазнала певної еволюції, то в Україні загальноприйнятим є поняття захисту інформації в інформаційно-телекомунікаційних системах, його найбільше використовують у законодавчих та нормативних документах.

Під тією або іншою інформаційною системою варто розуміти наступне:

– інформаційно-телекомунікаційна система – це організаційно-технічна система, яка реалізує певну сукупність технологій обробки та передавання даних шляхом їх кодування у формі фізичних сигналів;

– комп'ютерна система – це сукупність програмно-апаратних засобів, яку

подають на оцінювання (під оцінюванням слід розуміти експертне оцінювання захищеності інформації у цих програмно-апаратних засобах, при чому воно є складовою частиною експертизи на відповідність чинним нормативним документам та стандартам);

– обчислювальна система – це сукупність програмно-апаратних засобів, які призначені для оброблення інформації (така система поєднує у собі технічні засоби обробки та передавання інформації, а також методи й алгоритми обробки даних, які реалізовано у вигляді відповідного програмного забезпечення);

– автоматизована система – це організаційно-технічна система, яка реалізує інформаційну технологію та поєднує в собі: обчислювальну систему, фізичне середовище, персонал та оброблювальну інформацію.

В Україні, відповідно до нормативних документів Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ (НД ТЗІ 2.5-005-99) діє наступна класифікація автоматизованих систем:

– АС-1 – одномашинний однокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності (автономний/ізольований персональний комп'ютер, доступ до якого здійснюється з дотриманням організаційних засобів безпеки);

– АС-2 – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності (локальна обчислювальна мережа, яка відрізняється від попередньої категорії наявністю категорій користувачів з різними повноваженнями доступу та наявність апаратного забезпечення, яке може одночасно обробляти інформацію різних категорій конфіденційності);

– АС-3 – розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності (глобальна мережа, яка відрізняється від попередньої категорії тим, що передавання інформації відбувається через незахищене середовище).

Класифікація загроз для інформації та їх джерел. Концепція технічного захисту інформації в Україні визначає наступні джерела загроз для інформації: інші держави; політичні партії; злочинні угрупування; суб'єкти підприємницької діяльності; окремі фізичні особи; навмисні та ненавмисні дії персоналу; стихійні лиха та техногенні катастрофи.

Щодо мотивації цих джерел, то вона може бути зовсім різною: від повної її відсутності (стихійні лиха) до економічних та політичних переваг (табл. 3.1).

На основі цієї класифікації джерел можна сформувати одну із можливих класифікацій загроз для інформації (табл. 3.2).

Таблиця 3.1 – Джерела загроз для інформації

Джерела	Мотивація
Інші держави	Одержання переваг у зовнішньополітичній, зовнішньоекономічній, військовій, та інших сферах
Політичні партії	Одержання переваг у політичній боротьбі, боротьбі за владу
Злочинні угрупування	Одержання політичних, економічних переваг, нанесення шкоди
Суб'єкти підприємницької діяльності	Одержання переваг у конкурентній боротьбі, економічні переваги
Фізичні особи	Самоствердження, отримання економічних переваг і винагород
Помилки персоналу	Низька кваліфікація працівників; образа, зрада, примушення
Стихійні лиха, техногенні катастрофи	Не мають мотивації

Враховуючи теорію захисту інформації, якщо система захисту побудовано з урахуванням усіх сучасних методів та засобів захисту, тобто повністю реалізовано п. 3 таблиця 3.2, а підприємство має ретельно підібраний та навчений персонал, який не допускає помилок (повністю реалізовано п. 4 табл. 3.2), то навмисні дії порушників у такій системі неможливі.

Однак насправді це не зовсім так. З часом система захисту старіє, персонал змінюється або втрачає пильність, а зловмисники знаходять нові способи атак та методи подолання захисту, які були невідомими на час розробки цієї системи захисту. Тому, забезпечуючи обґрунтовану ступінь стійкості системи захисту інформації, слід пам'ятати про основне правило захисту інформації: жодна система захисту не може тривалий час протистояти цілеспрямованим діям «озброєного» сучасними технологіями кваліфікованого порушника.

Дане правило сформоване з набутого досвіду фахівців із захисту інформації та володіє універсальним характером. Воно не залежить від рівня системи захисту, сумлінності користувачів та адміністраторів, апаратного та програмного забезпечення. Воно говорить про те, що проблема полягає не в тому, чи подолають зловмисники систему захисту, а в тому, коли це відбудеться. А завдання захисту інформації полягає в тому, щоб злам системи відбувся якомога пізніше.

Спираючись на Концепцію технічного захисту інформації встановлюємо основну мету захисту інформації: унеможливлення або суттєве утруднення

реалізації загроз для інформації, що є власністю держави, сприяння реалізації законних інтересів громадян, юридичних осіб, державних органів здійсненню ними своїх завдань і функцій, загроз, реалізація яких може нанести державі, суспільству або особі політичні, економічні, моральні та інші збитки.

Таблиця 3.2 – Класифікація загроз для інформації

№ з/п	Загрози	Методи боротьби
1	Наслідки стихійних лих і техногенних катастроф	Резервування апаратного забезпечення (дзеркальні файлові та web-сервери, географічно рознесені); резервні копії інформації
2	Відмови обладнання	Резервування апаратного забезпечення (з можливістю «гарячої» заміни); резервні копії інформації; вибір надійного постачальника апаратного забезпечення; вчасна профілактика та ремонт апаратного забезпечення
3	Наслідки помилок проектування системи захисту	Залучення ліцензованих спеціалістів (ліцензіатів) для побудови та експертизи системи захисту; обов'язкова експертиза проекту; періодичний аудит системи захисту
4	Наслідки помилок персоналу	Ретельне підбирання персоналу; навчання персоналу; створення системи адміністративних стягнень за порушення; створення позитивного мікроклімату в колективі
5	Навмисні дії порушників	Залежно від способу дій

До основних завдань захисту інформації, виходячи з її мети, належать:

– захист інформації з обмеженим доступом від її витоку;

– протидія технічній розвідці;

– захист інформації з обмеженим доступом від несанкціонованої дії під час її оброблення та зберігання;

– захист інформації від спеціальних впливів;

– захист цілісності та доступності відкритої інформації.

Основні задачі, які повинні вирішуватися системою комп'ютерної безпеки. До основних задач, які повинні вирішуватись системою комп'ютерної безпеки слід віднести:

– керування доступом користувачів до інформаційних ресурсів з метою захисту від неправомірного випадкового або навмисного втручання у роботу системи і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів із боку персоналу та/або сторонніх осіб;

– захист даних, які передаються каналами зв'язку;

– реєстрування, збереження і надання даних про події, що відбувалися у системі і мали відношення до безпеки;

– контроль роботи користувачів системи з боку адміністраторів, обов'язкове повідомлення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;

– забезпечення замкненості програмного середовища із метою захисту від безконтрольного впровадження у систему потенційно небезпечних програм і засобів подолання системи захисту;

– керування засобами захисту.

Класифікація основних засобів протидії загрозам безпеки. Основні засоби протидії загрозам безпеки в інформаційних системах поділяють на правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні, технічні.

До правових засобів захисту слід віднести законодавчо-праву базу, на якій ґрунтуються інші засоби. Зокрема, це Закон України «Про інформацію», «Про технічний захист інформації», «Про державну таємницю» й нормативні документи Державної служби спеціального зв'язку та захисту інформації, які регламентують правила оброблення інформації.

До морально-етичних засобів протидії прийнято відносити дотримання норм поведінки, що традиційно склались або складаються в інформаційному суспільстві країни та світу.

Організаційні (адміністративні) засоби захисту – це засоби організаційного характеру, які, зазвичай, регламентують процес функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою, щоб унеможливити або максимально ускладнити здійснення загроз безпеки інформації.

Фізичні засоби захисту ґрунтуються на використанні різного роду механічних, електро- або електронно-механічних пристроїв, які призначені спеціально для створення фізичних перешкод на можливих шляхах проникнення потенційних порушників, їх доступу до компонентів системи та інформації, яка

захищається, а також засоби візуального спостереження, зв'язку і охоронної сигналізації.

Технічні (апаратно-програмні) засоби захисту базуються на використанні різних електронних пристроїв і спеціального програмного забезпечення, що входять до складу автоматизованої системи і виконують, самостійно або в комплексі з іншими засобами, функції захисту інформації.

3.2 Методи проведення атак на інформацію

Хакінг – внесення змін у програмне забезпечення для досягнення певної мети, яка відрізняються від цілей розробників програм (зазвичай вини шкідливі).

Людину, яка займається хакінгом, прийнято називати хакером. Це зазвичай досвідчений програміст. Проте існують й інші хакери, які мають більш небезпечні мотиви, ніж просто демонстрація своєї майстерності. Вони спрямовують свої знання на крадіжку особистої інформації, несанкціонований доступ тощо.

Хакінг – є серйозною проблемою індустрії. Він отримав величезний розвиток після створення мережі Інтернет через легкість доступу до комп'ютерів у будь-якій точці світу.

Злом програмного забезпечення – дії, спрямовані на усунення захисту програмного забезпечення, вбудованої розробниками для обмеження функціональних можливостей (останнє необхідно для стимуляції покупки такого програмного забезпечення, після якої обмеження знімаються).

Крек – програма, яка дозволяє здійснити злом програмного забезпечення. Зазвичай крек придатний для масового використання. По суті, крек є втіленням одного з видів злому, найчастіше – це звичайний патч.

Практично будь-який злом зводиться до використання одного з таких способів: серійний номер; реєстраційний код; генератор ключів; завантажувача; бінарний патч; емулятор ключа; підміна офіційного сайту програм і/або відповідна зміна налаштувань.

Введення серійного номера – злом програми за допомогою введення правильного реєстраційного ключа (або фрази), отриманого нелегальним способом. Ключ може генеруватися на основі будь-якої інформації (імені власника, характеристик апаратної частини комп'ютера тощо), або мати фіксоване значення. Для генерації реєстраційного ключа використовують той самий алгоритм, що і в програмі.

Реєстраційний код може поширюватися в ключовому файлі, який зазвичай розташовують у каталозі із встановленою програмою.

З метою масового злому, найчастіше створюють (і в подальшому використовують) генератор ключів – програма для генерації реєстраційних ключів. Цей вид злому найбільш затребуваний. Ключ генерується на основі якоїсь інформації і тому найбільш цінується. Зазвичай вимагає більшої кваліфікації зловмисника порівняно з іншими видами злому, але не завжди.

Використання завантажувача – спосіб обходити деякі види захисту програмного забезпечення (ПЗ), які полягають у використанні зовнішніх (навісних) систем захисту. Полягає у зміні певних фрагментів програми в оперативній пам'яті відразу після її завантаження в цю пам'ять, але перед її запуском (тобто перед виконанням коду в точці входу).

Застосування бінарного патча – спосіб, схожий на «завантажувач», але модифікація виробляється статично в файлах програми. Зазвичай це один із найпростіших і швидких способів злому ПЗ. Використання зламаної версії файлу – спосіб полягає в підміні оригінальних файлів програми файлами, які вже зламані.

Використання емулятора ключа – спосіб використовують для обману захистів, побудованих на використанні захисту електронного ключа, який під'єднують до LPT або USB порту. Полягає в знятті дампу внутрішньої пам'яті ключа. Файл із вмістом цієї пам'яті подається на вхід спеціальною програмою – емулятора, яка під'єднує свій драйвер-фільтр у стек драйверів і обманює захищену програму, емулюючи роботу з апаратним ключем. У разі наявності в програмі звернень до ключа для апаратного шифрування ділянки пам'яті цей метод використовують у зв'язці з методом Бінарний патч.

Підміна офіційного сайту програм і/або відповідна зміна налаштувань із метою обійти перевірку ключа, якщо вона була винесена розробниками на будь-який інтернет-ресурс (в абсолютній більшості випадків – для запобігання злому, рідше – для обліку і ведення статистики, збирання відомостей). Найчастіше здійснюється на примітивному рівні шляхом модифікування файлу «hosts» і запуску різних емуляторів, іноді – використання різних програм або використання реально існуючого веб-ресурсу.

Заборона доступу програми до інтернету полягає в комплексі дій, спрямованих на здійснення примусової заборони доступу програми до інтернету. Виконується в тому разі, коли програма вимагає активації ліцензійного ключа через інтернет (зазвичай офіційний сайт розробника), або у разі, коли програма зв'язується з сервером розробника для обміну даними або поновлення. Зазвичай, установлюється спеціальна утиліта, яка блокує доступ програми в мережу Інтернет, більш примітивний спосіб – фізичне відключення

від інтернету. Ця дія зазвичай проводиться після введення ключа, згенерованого кейгеном.

Скачування з інтернету або з іншого комп'ютера вже зламаної або купленої гри. Перекачування ліцензійної копії гри з одного комп'ютера зломом не є, але суть та сама.

Під часу злому складних захистів, а також за необхідності досягти максимального ефекту, застосовується комбінація перерахованих вище способів. В окремих випадках це відбувається під час недостатньої кваліфікованості зловмисника.

Цей список не є вичерпним, а лише позначає найчастіші способи злому.

Вид злому здебільшого обумовлений видом захисту. Для деяких захистів можна використовувати різні види злому, для інших – спосіб може бути єдиним.

Фрикінг – сленговий вираз, що означає злом телефонних автоматів, телефонних мереж і мереж мобільного зв'язку, з використанням прихованих від користувача або недокументованих функцій. Зазвичай фрикінг здійснюється для безкоштовних дзвінків, поповнення особистого мобільного рахунку.

Згодом внутрішньо-канальна службова міжстанційна сигналізація, яку часто зламували фрикери, була витіснена в загальні канали, відокремлені від потоку передачі голосу (CCS, Common Channel Signalling), зокрема у вигляді ОКС7 (SS–7, CCITT Signalling System № 7), і багато фрикінг-пристрої втратили можливості незаконного втручання в міжкомутаторну сигналізацію для вчинення актів шахрайства з оплатою голосових викликів.

3.3 Класифікація методів і засобів захисту інформації

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. Водночас компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз.

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовують шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, під час якої виключено витрати через недбалість і успішно відображено різні види загроз. Під перешкодою розуміємо спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифрування потрібне знання принципу.

Управління – способи захисту інформації, за яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус – методи захисту інформації, тісно пов'язані з регламентацією, що припускають введення комплексу заходів, за яких працівники змушені виконувати встановлені правила. Коли використовують способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісних міркувань, то йдеться про спонукання. Способи захисту інформації передбачають використання певного набору засобів.

Для запобігання втрати та витоку таємних даних використовують такі засоби: фізичні; апаратні; програмні; апаратно-програмні; законодавчі; криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів. Вони реалізуються на базі засобів обчислювальної техніки, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, які захищаються.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які монтуються в серійні блоки електронних систем оброблення та передавання даних для внутрішнього захисту засобів обчислювальної техніки: пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засоби, які засновані на синтезі програмних та апаратних засобів.

Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, які охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу.

3.4 Інформація з обмеженим доступом

Відповідно до ДСТУ 3396.0-96 будь-якій інформації властивий захист. Аналіз властивостей інформації, які потребують захисту, вказує на два її види:

– відкрита інформація, тобто така, яка призначена для ознайомлення усіх бажаючих (наприклад, газети, журнали, телевізійне та радіомовлення, інформаційні сайти, реклама тощо);

– інформація з обмеженим доступом, тобто така, ознайомитися з якою можна лише із дозволу її власників або розпорядників.

Згідно чинних нормативних документів, інформація із обмеженим доступом являє собою інформацію, права доступу до якої обмежено існуючими правилами та нормами.

На практиці інформацію з обмеженим доступом поділяють на такі категорії: конфіденційна та таємна.

Конфіденційною інформацією прийнято називати таку інформацію з обмеженим доступом, якою володіють, користуються або розпоряджаються окремі фізичні або юридичні особи чи держава, при цьому, порядок доступу до неї встановлюється ними.

Таємна інформація – це інформація з обмеженим доступом, яка містить відомості, які становлять державну або іншу передбачену чинним законодавством таємницю.

Віднесення інформації до категорії таємної відбувається згідно до чинного законодавства України. Отже, відмінність конфіденційної інформації від таємної полягає в тому, що остання захищається Законом України «Про державну таємницю», тому зловмисник, який несанкціоновано здобув або розголосив цю інформацію, автоматично завдає шкоди державі, суспільству або особі, і буде нести відповідальність відповідно до чинного законодавства. До конфіденційної інформації, як правило, відносять інформацію професійного, ділового, виробничого, банківського, комерційного та іншого характеру, яка не порушує передбаченої законом таємниці. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої є загрозою життю і здоров'ю людей.

Відповідно до Закону України «Про державну таємницю», державною таємницею вважають такий вид інформації, який охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній

безпеці України, та які визнано у порядку, встановленому цим законом і підлягають захисту держави.

Цим же ж законом визначено ступеня секретності інформації в Україні. У свою чергу, ступінь секретності інформації – це категорія, яка характеризує важливість таємної (секретної) інформації, степінь обмеження доступу до неї та рівень її охорони державою. Законом передбачається чотири ступені секретності:

– особливої важливості: детальні дані перепису населення, стратегічні плани Генерального штабу Збройних сил України; стратегічні політичні плани уряду тощо.;

– цілком таємно: детальні тактико-технічні дані передової військової техніки та технологія їх виробництва, плани розгортання військ; стратегічні плани парламентських партій та фракцій тощо;

– таємно: технологія виробництва військової техніки та її компонентів, стратегічні та тактичні плани військ та армійських підрозділів тощо;

– для службового користування (дана категорія секретності вказує на те, що такою інформацією можна вільно користуватися в межах підприємства, але вона не підлягає розголошенню за його межами): фінансова звітність підприємства, дані про заробітну платню його працівників, про структуру постачання, можуть бути також дані про збут.

Враховуючи Закон України «Про захист персональних даних» (чинний від 01.01.2011), персональні дані особи, використання яких може однозначно ідентифікувати людину, відносять до категорії секретності «Для службового користування».

3.5 Структура політики безпеки та її основні частини

Політика безпеки організації – сукупність принципів, правил, процедур і практичних рішень у галузі безпеки, які регулюють керування, захист та розподіл інформації, що захищається.

Політика безпеки (ПБ) залежить від багатьох чинників, а саме:

– від рівня секретності та властивостей інформації, яка підлягає захисту;

– від конкретної технології обробки інформації;

– від технічних та програмних засобів, що використовуються організацією;

– від розташування організації; інших чинників, які уточнюються на етапі розробки політики безпеки.

Політика безпеки повинна враховувати сучасний стан та найближчі

перспективи розвитку інформаційних технологій, мету, завдання, правові основи експлуатації, режими функціонування об'єктів, містити аналіз загроз безпеки та способи їх реалізації.

Основні положення ПБ повинні розповсюджуватися на усі структурні підрозділи організації, а також на інші організації, які взаємодіють з основною організацією як постачальники або споживачі інформаційних ресурсів.

Законодавчою основою ПБ є Конституція України, Цивільний та Карний кодекси України, Закони, Постанови, документи Держспецзв'язку тощо.

Політика безпеки є методологічною основою для:

– формування та впровадження єдиної політики в галузі захисту інформації організації;

– прийняття важливих рішень та розробки спільних практичних заходів, спрямованих на виявлення, знешкодження та ліквідацію наслідків реалізації різних типів загроз безпеці інформації;

– координації діяльності структурних підрозділів організації при виконанні робіт зі створення, розвитку та експлуатації інформаційних ресурсів з дотриманням вимог із забезпечення інформаційної безпеки;

– розробки пропозицій щодо вдосконалення правового, нормативного, технічного та організаційного забезпечення інформаційної безпеки в організації.

При розробці ПБ враховують основні принципи створення комплексних систем забезпечення безпеки, характеристики та можливості організаційно-технічних методів, сучасні апаратно-програмні засоби захисту та протидії загрозам безпеці інформації.

Політика безпеки, як правило, складається із нижченаведених розділів.

1. Загальні положення (обговорюють призначення та правову основу цього документу, подають основні визначення та термінологію).

2. Об'єкти захисту (описують категорії інформаційних ресурсів, які підлягають захисту, подають структуру, склад і розміщення основних об'єктів захисту та інформаційні зв'язки між ними).

3. Мета та основні завдання забезпечення безпеки (описують інтереси суб'єктів інформаційних відносин, які об'єднані розробкою ПБ, мету й основні завдання системи забезпечення безпеки організації та шляхи вирішення поставлених завдань).

4. Основні загрози безпеки інформації організації (описують основні загрози та шляхів їх реалізації). Як правило, загрози поділяються на природні та штучні або суб'єктивні. Штучні загрози поділяються на навмисні та ненавмисні. Усі загрози, як правило, описуються в рамках так званої моделі загроз –

формалізованого або неформалізованого опису можливих загроз та шляхів їх реалізації. Неформалізований опис загроз – опис у вигляді звичайного тексту; формалізований – із залученням таблиць, графіків, математичних моделей. Для найбільш відповідальних випадків використовують математичні моделі загроз, які повинні довести адекватність та повноту обраних типів загроз та шляхів їх реалізації.

5. Модель можливих порушників (подають формальний або неформальний опис порушника, його мотивації, кваліфікацію та можливі дії). Для найбільш відповідальних випадків будують математичну модель порушника, яка доводить свою повноту і адекватність в умовах роботи.

6. Витік інформації технічними каналами (аналізують можливі існуючі та майбутні технічні канали витоку інформації та описують активні та пасивні способи протидії).

7. Основні принципи побудови системи інформаційної безпеки організації (описують законність, системність, комплексність, неперервність захисту, модифікованість, економічну доцільність, персональну відповідальність, мінімізацію повноважень, розмежування функцій, гнучкість та простоту системи захисту, обґрунтування та можливість технічної реалізації розробленої ПБ). Зазвичай акцентують увагу на описі методів контролю та їх обов'язковості.

8. Методи та засоби забезпечення задекларованого рівня захищеності інформаційних ресурсів (описують засоби забезпечення інформаційної безпеки, зокрема, регламентують доступ до приміщення, допуск співробітників до інформаційних ресурсів; порядок обслуговування та модифікацію апаратних та програмних ресурсів). В даному розділі регламентують методи забезпечення фізичної цілісності (незмінності конфігурації) апаратних та програмних ресурсів. Описують методи підбору та підготовки персоналу, його відповідальність за порушення встановленого порядку користування інформаційними ресурсами підприємства. Окремим підпунктом прописують засоби забезпечення інформаційної безпеки підприємства: фізичні та технічні засоби захисту; засоби ідентифікації та автентифікації користувачів, засоби обмеженого доступу; засоби контролю та реєстрації подій (аудит) в системі; криптографічні засоби захисту.

9. Порядок внесення змін та доповнень (регламентують порядок внесення змін та доповнень до ПБ).

Варто пам'ятати, що основою будь-якої ПБ є модель загроз та модель порушника. Разом із рівнем секретності інформації, яку необхідно захищати, вони визначають і витрати як на створення системи захисту, так і ПБ.

3.6 Життєвий цикл розробки систем безпеки

Розроблення профілю захисту і проекту безпеки об'єкта оцінки. У 1999 році було завершено розроблення міжнародного стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій», який більш відомий як «Єдині критерії». Даний стандарт дозволяє усунути концептуальні та технічні розходження, які були присутні у раніше розроблених нормативних документах й характеризує новий, міждержавний рівень стандартизації інформаційних технологій.

Однією із основних цілей цього стандарту є створення методологічної бази для здійснення оцінювання властивостей безпеки продуктів і систем інформаційних технологій. У розрізі проблеми забезпечення ІТ-безпеки розробники стандарту виходять з того, що є дві конфліктуючі сторони – власник ресурсів, який становить певну цінність та вимагає свого захисту, та зловмисник, який має на меті незаконне використання ресурсів, що може призвести до завдання збитків (морального, матеріального, економічного тощо) власнику ресурсів. При цьому під ресурсами розуміють не тільки інформацію (інформаційні ресурси), але й інші їх види. Зловмисника розглядають як джерело загроз безпеки – можливих подій, впливів, процесів або явищ, що є потенційною небезпекою, реалізація яких може призвести до завдання збитків власнику ресурсів. У зв'язку з цим власник ресурсів змушений вживати заходів, які спрямовані на запобігання або зменшення ступеня цих небезпек. У якості основних загроз розглядають загрози порушення конфіденційності, цілісності й доступності. Для ефективної протидії зловмиснику власником ресурсів складається якомога повніший перелік загроз, які можна реалізувати в конкретних умовах. Аналіз ризику реалізації загроз здійснюється шляхом завдання моделі порушника й оцінювання ймовірності реалізації тієї або іншої загрози. Отримані результати дають змогу сформувати вимоги щодо забезпечення ІТ-безпеки, реалізація яких сприяє зменшенню ризиків до прийнятного рівня.

Вимоги ІТ-безпеки по своїй суті містять у собі функціональні вимоги безпеки та вимоги адекватності. Функціональні вимоги безпеки визначають набір функцій безпеки, які реалізовують під час забезпечення конфіденційності, цілісності й доступності. Для того щоб механізм безпеки та засоби захисту її функцій, які реалізуються, можна було визнати ефективними, необхідно отримати високий ступінь впевненості у правильності їх вибору та надійності функціонування. Така впевненість досягається шляхом пред'явлення та реалізації вимог адекватності.

Основними об'єктами застосування вимог безпеки є ІТ-продукти і ІТ-системи. Під продуктом інформаційних технологій варто розуміти представлення кінцевому споживачу готового до використання апаратного, програмного або програмно-апаратного засобу (або сукупність таких засобів) обробки інформації. ІТ-продукт не призначений для автономної експлуатації й інтегрується в ІТ-систему (автоматизована система обробки інформації), яка становить організаційно-технічну систему, та містить у собі: сукупність технічних засобів передачі і обробки інформації (ІТ-продуктів), об'єднаних у функціонально повний комплекс; сукупність методів і алгоритмів обробки інформації у вигляді відповідного програмного забезпечення; інформаційні та інші ресурси; персонал і користувачів, об'єднаних за організаційно-структурним, тематичним, технологічним й іншими принципами для здійснення автоматизованої обробки інформації.

Практична реалізація вимог ІТ-безпеки виражається у розробленні продукту або системи захисту інформації. З поміж основних термінів стандарту ISO/IEC 15408 вирізняється об'єкт оцінки – ІТ-продукт або система, а також пов'язана з ними експлуатаційна, технічна, користувальницька та інша документація, яка є основним об'єктом перевірки і оцінки. Основними документами, які характеризують об'єкт оцінки з точки зору забезпечення ІТ-безпеки, є профіль захисту та проект забезпечення безпеки.

Порядок розроблення профілю захисту і проекту забезпечення безпеки. Профіль захисту (ПЗ) – це реалізаційно-незалежна множина функціональних вимог безпеки та вимог адекватності, які спрямовано на задоволення потреб споживача. Профіль захисту являє собою нормативний документ, який регламентує усі аспекти безпеки ІТ-продуктів й систем у вигляді сукупності функціональних вимог і вимог адекватності, що пропонуються функціям безпеки відносно механізмів захисту. На практиці ПЗ прийнято використовувати для класифікації об'єкта оцінки.

У свою чергу ПБ становить множину вимог безпеки та специфікацій її функцій. Проект безпеки використовується як основа для здійснення оцінювання розглянутого об'єкта оцінки. Окрім специфікацій функцій безпеки і засобів захисту ПБ містить і вимоги до сертифікації об'єкта оцінювання та підсумкову специфікацію системи (підсистеми) забезпечення безпеки в конкретному ІТ-продукті або системі. Розроблення таких документів є основним практичним додатком Єдиних критеріїв. Розроблення ПЗ і ПБ здійснюється у відповідності до наступних етапів:

– І етап – Аналіз безпеки середовища експлуатації об'єкта оцінювання;

– II етап – Визначення й формулювання завдань із забезпечення безпеки;

– III етап – Розроблення вимог IT-безпеки;

– IV етап – Розроблення специфікацій функцій безпеки й підсумкової специфікації забезпечення безпеки об'єкта оцінки.

Аналіз безпеки середовища експлуатації об'єкта оцінювання здійснюється для:

– обмеження системи (підсистеми) забезпечення безпеки об'єкта оцінювання від навколишнього середовища експлуатації;

– формування вихідних передумов для визначення завдань із забезпечення безпеки;

– визначення ступеня небезпеки (агресивності) середовища експлуатації для функціонування об'єкта оцінювання шляхом виявлення загроз безпеки і аналізу ризиків;

– середовище експлуатації становить сукупність фізичних, інформаційних, технічних об'єктів і систем, зовнішніх стосовно об'єкта оцінки, а також організаційних заходів, правових норм, умов експлуатації і технологічних особливостей застосування об'єкта оцінювання, які здійснюють фізичний, інформаційний, енергетичний та інший вплив на функціонування об'єкта оцінки (сюди входять також й можливі загрози безпеки, які вже існують або можуть виникнути в даному середовищі).

Результатами аналізу безпеки є:

– аксіоматичні висновки (припущення) про безпеку середовища експлуатації конкретного об'єкта оцінки;

– перелік загроз безпеки, оцінка ймовірності їх реалізації і модель порушника безпеки (кожна загроза характеризується із трьох сторін: визначається модель порушника безпеки, що здатний реалізувати конкретну загрозу; описуються передбачувані методи нападів (атак) і можливі слабкі місця (уразливості) системи, використання яких покладено в основу реалізації атак);

– висновки щодо застосованості організаційної політики безпеки.

Під організаційною політикою безпеки слід розуміти одне або кілька правил, процедур, практичних заходів (дій) або загальних рекомендацій, спрямованих на забезпечення безпеки і експлуатації об'єкта оцінювання накладаються організацією відповідно до виконуваних даною організацією функцій.

На основі отриманих у ході аналізу безпеки середовища експлуатації результатів здійснюється визначення і формулювання задач із забезпечення безпеки або задач захисту.

Задача захисту – це цільова постановка задачі на протидію виявленим загрозам і задоволення політики безпеки. Задача захисту повинна бути погоджена із множиною інших функціональних задач об'єкта оцінювання та не суперечити основному призначенню цього об'єкта. Задачі визначаються як для об'єкта оцінювання, так і для середовища його експлуатації (причому останні формулюють тільки для елементів середовища експлуатації, які пов'язаних з інформаційними технологіями). Технічні засоби забезпечення безпеки, організаційні міри, правові норми розглядаються як зовнішні стосовно об'єкта оцінки елементи системи захисту, застосовувані для підвищення ефективності власних засобів забезпечення безпеки об'єкта оцінки.

Таким чином, задача захисту адресована винятково для реалізації вимог забезпечення ІТ-безпеки.

Сформульовані і, по можливості, формалізовані задачі захисту є базою для безпосередньої розробки профілю захисту. Розробка профілю захисту здійснюється у два етапи: пошук і вибір профілю прототипу; синтез вимог ІТ-безпеки.

Міжнародний стандарт передбачає створення спеціальної картотеки пакетів вимог безпеки, профілів захисту і проектів безпеки. Пакетом вимог називають проміжну комбінацію вимог безпеки, яка описує множину функціональних вимог і вимог адекватності, які забезпечують рішення виділеної підмножини задач захисту (ця картотека є доступною для розробників, що дозволяє мінімізувати витрати на розробку нових профілів захисту і врахувати досвід попередніх розробок).

Вимоги ІТ-безпеки є уточненням, конкретизацією і відображенням задач захисту в множині вимог безпеки, які пропонуються об'єкту оцінювання відносно його середовища експлуатації. Вимоги ІТ-безпеки містять у собі три компоненти:

- функціональні вимоги безпеки;
- вимоги адекватності;
- вимоги безпеки середовища експлуатації.

Під час розроблення профілю захисту здійснюється вибір вимог безпеки специфічних для конкретного середовища. При цьому вибір ґрунтується на оцінюванні ефективності вимог для рішення задачі протидії загрозам безпеки. Функціональні вимоги визначають властивості безпеки і характеризують функції об'єкта оцінки, які є типовими для підтримки ІТ-безпеки.

Демонстрація того, що виконання функціональних вимог веде до забезпечення необхідного рівня безпеки, здійснюється через включення в

профіль захисту вимог адекватності. Адекватність формується за двома аспектами: ефективність функцій безпеки; коректність реалізації функцій безпеки.

Під час оцінювання ефективності функцій безпеки визначають степінь відповідності між завданнями захисту й пропонованим набором функцій безпеки, їх функціональною повнотою, погодженістю, простотою використання і ступенем запобігання загрозам безпеки. Коректність виражається у вигляді оцінки правильності та надійності реалізації функцій безпеки (для конкретної множини функціональних вимог ступінь адекватності може варіюватися).

Розроблення профілю захисту вимагає аналізу зв'язків та взаємозалежностей між різними функціональними вимогами та вимогами адекватності.

Четвертий етап забезпечується рід час розроблення проекту безпеки. На даному етапі здійснюється розроблення підсумкової специфікації об'єкта оцінювання. Ця специфікація має містити опис заявлених функцій безпеки, які задовольняють функціональним вимогам і визначення показників адекватності, які характеризують степінь задоволення вимог адекватності.

Структура і зміст профілю захисту. Відповідно до стандарту ISO/IEC 15408-1 профіль захисту повинен містити наступні розділи:

– короткий опис профілю (містить класифікаційну інформацію, яка необхідна для ідентифікації в спеціальній картотеці; характеризується основне завдання або група завдань із забезпечення безпеки, які будуть розв'язані за допомогою цього профілю);

– короткий опис об'єкта оцінювання (формують призначення й область застосування об'єкта оцінювання; короткий опис особливостей, використовуваних у об'єкті оцінювання інформаційних технологій; короткий опис додатків, у яких передбачено використання об'єкта оцінювання);

– аналіз середовища експлуатації об'єкта оцінювання (містить результати аналізу безпеки середовища експлуатації об'єкта оцінки: висновки щодо різних аспектів безпеки середовища, в якому застосовано або передбачено застосування об'єкта оцінки; повний опис загроз безпеки, які безпосередньо впливають на безпеку об'єкта оцінки; опис організаційних політик безпеки);

– завдання із забезпечення безпеки (описують завдання захисту для об'єкта оцінювання і його середовища експлуатації: відображають конкретні цілі, що досягаються під час забезпечення безпеки; застосовуються з метою запобігання усіх виявлених загроз безпеки; охоплюють усі організаційні політики безпеки);

– вимоги ІТ-безпеки (описують функціональні можливості засобів захисту об'єкта оцінювання та визначають рівень адекватності висунутих функціональних вимог відносно певного раніше переліку загроз безпеки: функціональні вимоги безпеки для об'єкта оцінювання; вимоги адекватності безпеки об'єкта оцінювання; вимоги безпеки для ІТ-середовища експлуатації об'єкта оцінювання);

– обґрунтування завдань захисту і вимог ІТ-безпеки (подають докази того, що профіль захисту становить повну і зв'язну множину вимог до об'єкта оцінювання, які задовольняють висунуті вимоги та забезпечує ефективну протидію погрозам безпеки).

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Інформаційна система та захист інформації у ній.
2. Класифікація автоматизованих систем захисту інформації.
3. Класифікація загроз для інформації та їх джерел.
4. Основна мета та завдання захисту інформації.
5. Класифікація основних засобів протидії загрозам безпеки.
6. Хакінг. Крек. Фрикінг.
7. Класифікація методів та засобів захисту інформації.
8. Інформація з обмеженим доступом.
9. Ступені секретності.
10. Політика безпеки: методологічна основа та структура.
11. Життєвий цикл розробки системи безпеки.
12. Етапи розроблення програмного забезпечення та політики безпеки.
13. Компоненти вимог ІТ-безпеки.
14. Структура та зміст профілю захисту.

Література: [2; 5-11; 14-17].

Тема 4. Загрози інформаційної безпеки. Основні види атак, принципи криптоаналізу

План:

4.1 Загрози інформаційної безпеки

4.2 Атаки на інформаційні системи

4.3 Класифікація атак на симетричні та асиметричні криптоалгоритми

4.4 Механізми захисту від атак

4.5 Диференціальний криптоаналіз

4.6 Лінійний криптоаналіз

4.1 Загрози інформаційної безпеки

Загроза інформаційної безпеки – сукупність умов та чинників, які створюють небезпеку порушення інформаційної безпеки.

Під загрозою (для загального випадку) необхідно розуміти потенційно можливу подію, дію/вплив, процес або явище, які можуть призвести до заподіяння шкоди будь-чиїм інтересам.

Під загрозою інтересів суб'єктів інформаційних відносин прийнято розуміти потенційно можливу подію, процес або явище, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або опосередковано призвести до заподіяння шкоди даним того чи іншого суб'єкта. Іншими словами загроза являє собою процес настання таких змін у стані особи, суспільства або держави, які оцінюються ними як здатність створювати перешкоди або унеможливити реалізацію їх інтересів.

Водночас термін «загроза» означає можливу небезпеку, тому припускає не лише процес настання змін, а й можливість їх настання. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого- або чого-небудь», «те, що може заподіювати будь-яке зло, якусь неприємність».

Під загрозою (для загального випадку) зазвичай розуміють потенційно можливу подію (дію, процес або явище), яка може призвести до нанесення збитків для будь-чиїх інтересів. Надалі, під загрозою безпеки автоматизованої системи (АС) оброблення інформації варто розуміти можливість впливу на АС, який прямо або побічно може завдати шкоди її безпеці.

На практиці відомою є інформація про великий перелік загроз інформаційної безпеки АС, які складаються із сотні позицій.

Розгляд можливих загроз інформаційної безпеки здійснюють із метою визначення повного набору вимог до розроблюваної системи захисту.

Перелік загроз, оцінювання ймовірностей їх реалізації, а також модель порушника є основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту АС. Окрім виявлення можливих загроз доцільним є проведення аналізу таких загроз на основі їх класифікації за низкою ознак. Кожна з ознак класифікації відображає одну із узагальнених вимог, які висуваються до системи захисту. У свою чергу загрози, які відповідають кожній із ознак класифікації, дозволяють деталізувати відображувану цією ознакою вимогу.

Необхідність у класифікації загроз інформаційної безпеки АС обумовлена тим, що інформація, яка зберігається та оброблюється у сучасних АС піддається

впливу надзвичайно великої кількості чинників, через що неможливо формалізувати задачу опису повної множини загроз. Зважаючи на це, для системи, яка захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Класифікацію можливих загроз інформаційної безпеки АС можна провести за нижченаведеними базовими ознаками.

1. За природою виникнення:

– природні загрози, які викликані впливами на АС об'єктивних фізичних процесів або стихійних природних явищ;

– штучні загрози безпеки АС, які викликані діяльністю людини.

2. За ступенем навмисності прояву:

– загрози, які викликані помилками або халатністю персоналу;

– загрози навмисної дії.

3. За безпосереднім джерелом загроз:

– природне середовище;

– людина;

– санкціоновані програмно-апаратні засоби;

– несанкціоновані програмно-апаратні засоби.

4. За розміщенням джерел загроз:

– поза контрольованої зони АС;

– у межах контрольованої зони АС;

– безпосередньо в АС.

5. За ступенем залежності від активності АС:

– незалежно від активності АС;

– лише під час оброблення даних;

6. За ступенем впливу на АС:

– пасивні загрози, які під час реалізації нічого не змінюють у структурі та змісті АС;

– активні загрози, які під час дії вносять зміни в структуру і зміст АС.

7. За етапами доступу користувачів або програм до ресурсів:

– загрози, які проявляються на етапі доступу до ресурсів АС;

– загрози, які проявляються після дозволу доступу до ресурсів АС;

8. За способом доступу до ресурсів АС:

– загрози, які здійснюють із використанням стандартного шляху доступу до ресурсів АС;

– загрози, які здійснюються із використанням прихованого нестандартного шляху доступу до ресурсів АС.

9. За поточним місцем розміщення інформації, яка зберігається та обробляється в АС:

– загрози доступу до інформації, яка розміщена на зовнішніх запам'ятовувальних пристроях;

– загрози доступу до інформації, яка розміщена в оперативній пам'яті;

– загрози доступу до інформації, яка циркулює в лініях зв'язку;

– загрози доступу до інформації, яка відображається на терміналі або надрукованої на принтері.

4.2 Атаки на інформаційні системи

Хакерська атака – спроба реалізації загрози, тобто – це дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під атакою на інформаційну систему розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційних ресурсів, шляхом використання вразливостей цієї ІС.

Типи атак на інформаційні системи:

– віддалене проникнення (remote penetration);
– локальне проникнення (local penetration);
– атака на відмову під час обслуговування (denial of service);
– мережні сканери (network scanners);
– сканери вразливостей (vulnerability scanners);
– зламувачі паролів (password crackers);
– аналізатори протоколів (sniffers);
– спам e-mail (Mailbombing);
– перехоплення каналу зв'язку (Man-in-the-Middle).

Віддалене проникнення. Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. До прикладів програм, які реалізовують цей тип варто віднести: NetBus та BackOrifice.

NetBus або Netbus – програма дистанційного керування комп'ютерною системою Microsoft Windows по мережі, яка має клієнт-серверну архітектуру.

BackOrifice – комп'ютерна програма, яка дозволяє віддалене адміністрування системи (дозволяє керувати декількома комп'ютерами одночасно, використовуючи їх образи).

Локальне проникнення. Атака, яка призводить до отримання несанкціонованого доступу до вузла інформаційно-комунікаційних систем і

мереж (ІКСМ), на якому вона запущена. Прикладом такої програми є GetAdmin.

GetAdmin.exe це різновид файлу «EXE», який пов'язано із Guide to Hacking Software Security 2002 розроблений Silver Star Publishing для ОС Windows.

Файли «EXE» (виконання), такі як GetAdmin.exe – це файли, які містять покрокові інструкції, котрими комп'ютер користується, щоб виконати ту чи іншу функцію. Коли запускається файл з розширенням «EXE», то комп'ютер автоматично виконує ці інструкції, які створено розробником програми, з метою запуску програми.

Кожен програмний додаток використовує файл виконання: веб-браузер, текстовий редактор, програма для створення таблиць тощо. Це робить ці файли одними із найбільш корисних видів файлів ОС.

Через свою корисність і наполегливість файли «EXE» зазвичай використовують як спосіб зараження вірусами (шкідливим ПЗ). Найчастіше віруси маскуються під безпечні файли «EXE» (наприклад, GetAdmin.exe) і поширюють через поштовий СПАМ або шкідливі веб-сайти, що призводить до зараження комп'ютера.

Варто зауважити, що віруси можуть заразити, перемістити або пошкодити існуючі файли «EXE», що, в подальшому, призводить до формування повідомлення про помилки під час виконання пов'язаних програм. Отже, будь-який файл виконання, який завантажується на комп'ютер, необхідно перевірити на віруси перед відкриттям, навіть у тому випадку коли він отриманий з надійного джерела.

Помилки «EXE», які пов'язані із GetAdmin.exe, найчастіше з'являються під час запуску комп'ютера, запуску програми або під час спроби використання специфічних функцій програми.

Повідомлення про наявні помилки «EXE» можуть з'являтися під час встановлення програми, якщо вона пов'язана із GetAdmin.exe, під час запуску або завершення роботи Windows, або навіть під час встановлення ОС Windows.

При цьому відстеження моменту появи помилки GetAdmin.exe є важливою інформацією під час усунення цієї проблеми.

Атака на відмову під час обслуговування. Розподілена атака на відмову під час обслуговування (DoS attack, DDoS attack, Denial-of-service attack) – це напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих), таким чином, атаковане

устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним.

Відмову сервісу прийнято здійснювати за допомогою:

– примусу атакованого устаткування до зупинення роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;

– зайняття комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам (рис. 4.1).

На сьогодні існує достатньо багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або вразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосереднього пересилання великої кількості пакетів (SYN, UDP, ICMP flood), використання проміжних вузлів (Smurf, Fraggle), передавання занадто довгих пакетів (Ping of Death), некоректних пакетів (Land) або великої кількості трудоємних запитів.

Зауважимо, що впродовж останнього часу відбувається бурхливий розвиток цього напряму діяльності та поява нових видів і способів атак. З останніх тенденцій можна відзначити появу атак погіршення якості (Quality Reduction Attack) та низькочастотних атак (Low Rated Attack) і, безумовно, цей процес буде продовжуватися, потребуючи нових досліджень і розроблення нових методів протидії.

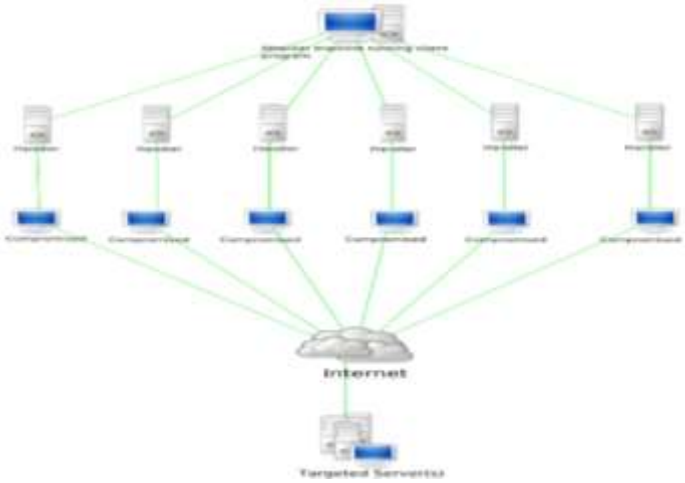

Рисунок 4.1 – DoS attack (атака на відмову під час обслуговування)

Відзначимо, що на сьогодні, основні класи атак вивчені достатньо добре. Однак, на практиці, спостерігаються різні підходи до їх класифікації. Під час роботи атаки класифікують за протоколами, відносно яких вони здійснюються. Розрізняють наступні атаки: SYN flood, TCP reset, ICMP flood, UDP flood, DNS request, CGI request, Mail bomb, ARP storm і атаки на алгоритмічну складність (рис. 4.2).

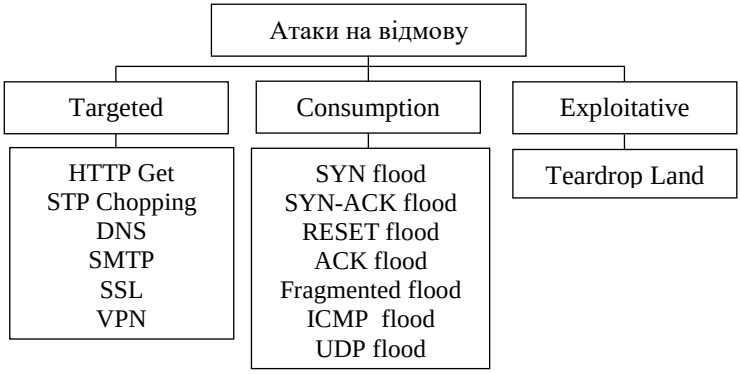

Рисунок 4.2 – Класифікація атак на відмову (Prolexic Technologies)

4.3 Класифікація атак на симетричні та асиметричні криптоалгоритми

У минулому, коли сторонами, які обмінювалися конфіденційною інформацією, були переважно дипломати та військові, можна було бути впевненими у надійності учасників обміну, довіряти один одному. Основною проблемою сторін того часу було забезпечення неможливості втручання у конфіденційний зв'язок третіх сторін. Практично не зустрічалися випадки, коли адресати поводили себе недобросовісно: відмовлялися від отриманих повідомлень або стверджували про якісь зміни у їх текстові. Основне завдання тогочасних криптографів полягало лише у забезпеченні конфіденційності інформації.

Принципово протилежною є ситуація на сьогодні, коли інформацією обмінюються суб'єкти комерційної діяльності, які можуть не довіряти один одному. І якщо раніше важливо було забезпечити лише конфіденційність інформації, то зараз не менш важливо забезпечити її цілісність та юридичну чинність, а також захиститися від нав'язування хибних повідомлень.

Отже, метою суб'єкта в такому разі є перешкоджання здійсненню намірів законних учасників інформаційного обміну. В загальному випадку зловмисник може не лише перехоплювати зашифровані повідомлення, але й модифікувати

їх, а також направляти фальсифіковані повідомлення легальним сторонам, що обмінюються інформацією, ніби від імені їх легальних партнерів.

Таким чином, існує чотири можливі типи загроз з боку зловмисників:

– порушення конфіденційності інформації (дешифрування, повне або часткове передання повідомлення або отримання додаткової інформації про його зміст);

– порушення цілісності інформації (внесення змін у повідомлення, які змінюють його зміст);

– забезпечення неможливості відмови від отриманого або відправленого повідомлення;

– порушення істинності повідомлень (формування хибних повідомлень, які легальні учасники інформаційного обміну можуть класифікувати як істинні).

Дешифрування перехопленого повідомлення можливе лише у випадку обчислення криптографічного ключа або так званого «безключового читання», тобто за допомогою знаходження еквівалентного алгоритму, що не вимагає знання ключа.

Процес, при якому реалізується спроба отримати відкритий текст, ключ або і те, і інше, називається криптоаналізом. Однією з можливих атак на алгоритм шифрування є атака грубою силою (лобова атака), тобто просте перебирання усіх можливих ключів. Якщо кількість ключів досить велика, то підібрати потрібний дуже складно. При довжині ключа n бітів кількість можливих ключів дорівнює 2n. Таким чином, чим довшим є ключ, тим стійкішим вважається алгоритм для лобової атаки.

Існують різні типи атак, які ґрунтуються на тому, що зловмиснику відома певна кількість пар відкритого тексту-шифротексту. Під час аналізу зашифрованого тексту зловмисник часто застосовує статистичні методи аналізу тексту. При цьому він має загальну уяву про тип тексту (наприклад, мова написання тексту, .exe-файл конкретної операційної системи, вихідний текст мови програмування тощо). У деяких випадках криптоаналітик володіє великою кількістю інформації про відкритий текст і може перехоплювати одне або кілька незашифрованих повідомлень разом із їх шифротекстом. В окремих випадках він може знати про основний формат або основні характеристики повідомлення.

В усіх випадках прийнято вважати, що криптографічна схема є безпечною, якщо зашифроване повідомлення не містить ніякої інформації про відкритий текст. Схема буде обчислювально безпечною, якщо:

– вартість розшифрування повідомлення більша від вартості інформації у відкритому повідомленні;

– час, який необхідно для розшифрування повідомлення, буде більшим за період життя повідомлення.

Класифікація атак на симетричні криптоалгоритми. Охарактеризуємо основні типи атак у порядку зростання небезпеки.

1. Атака на основі шифротексту (ciphertext-only-attack). У даному випадку зловмиснику відомо лише про шифротексти, які зашифровано одним ключем. Це найслабший тип криптоаналітичної атаки, успіх якої зовсім неочевидний. Він залежить від багатьох чинників та визначається кваліфікацією аналітика (за умови ручного криптоаналізу) або повністю визначається потужністю комп'ютерів криптоаналітичної системи.

Завжди процес криптоаналізу починається зі збирання інформації про відкритий текст:

– якою мовою написаний оригінал;
– які лінгвістичні особливості цієї мови;
– які слова або фрази може містити оригінал та у якій послідовності;
– якою приблизно може бути довжина оригінального тексту;
– які методи шифрування могли застосувати для шифрування цього тексту;
– яка службова інформація може міститися у тексті (дата, контрольна сума, адреси тощо);
– якою апаратурою було зашифровано текст.

Ці або схожі дані збираються агентурними або аналітичними засобами і значно полегшують роботу криптоаналітиків.

2. Атака на основі невибраного (відомого) відкритого тексту (known-plaintext attack). Зловмисник знає або може встановити деякі частини відкритого тексту у криптограмі. Завдання полягає в тому, щоб дешифрувати увесь текст. Це можна виконати шляхом покрокового обчислення ключа.

3. Атака на основі обраного відкритого тексту (chosenplaintext attack). Зловмисник може обрати будь-який відкритий текст і отримати для нього зашифрований. Завдання полягає у визначенні ключа шифрування. Деякі алгоритми шифрування досить вразливі для атак цього типу. Тому у випадку використання таких систем, серйозної уваги вимагає внутрішня безпека використання системи, щоб зловмисник ні в якому разі не зміг отримати доступ до відкритих текстів.

Така атака буде називатися простою в разі, коли усі відкриті тексти зловмисник отримує до перехоплення першої криптограми, та адаптивною, коли зловмисник обирає черговий відкритий текст, маючи шифровки усіх попередніх.

4. Атака на основі обраного шифротексту (chosen-ciphertext attack). Зловмисник може обирати потрібну кількість криптограм та отримати для них відкриті тексти. Тут також, аналогічно до попереднього типу атак, існують різновиди простої та адаптивної атак.

5. Атака на основі обраного тексту (chosen-text attack). Це найнебезпечніший тип атак, оскільки зловмисник може передавати спеціально підготовлені відкриті тексти для шифрування, а потім отримувати відповідні шифровки. Завдання полягає у розкритті ключа. Ця атака також може бути простою та адаптивною.

Якщо зловмисник здійснює атаку на основі лише шифротексту, у нього є дуже обмежений набір можливостей. До них можна віднести метод грубої сили або частотний криптоаналіз.

У разі атаки на основі відомого відкритого тексту розкриття шифру буде примітивним після того, коли у текстах зустрінеться більшість літер абетки.

Якщо зловмисник має можливість атакувати на основі обраного тексту, то криптосистему буде розкрито вже після шифрування відкритого тексту.

Класифікація атак на асиметричні криптоалгоритми. Специфічний тип атаки – «посередництво» (Man-in-middle attack). Ця атака спрямована на зламування криптографічних комунікацій та протоколів обміну ключами. Атака здійснюється наступним чином: зловмисник (З), має змогу перехоплювати усі повідомлення сторін А та В. Припустимо також, що сторони хочуть обмінятися криптографічними ключами, тож А відправляє свій ключ шифрування $К_{АВ}$ стороні В. Зловмисник перехоплює цей ключ, зберігає його, та відправляє стороні В вже свій криптографічний ключ, $К_{ЗВ}$, ніби від сторони А. Сторона В, отримавши цей ключ, у відповідь відправляє стороні А свій криптографічний ключ $К_{ВА}$. Зловмисник також підміняє цей ключ своїм, КЗА і надсилає його стороні А. Таким чином, сторони А та В «вірять», що мають криптографічні ключі один одного, хоча насправді вони мають лише два різні ключі зловмисника З. Той, у свою чергу, має обидва ключі сторін та може читати усю їх зашифровану інформацію (рис. 4.3). Спроба обміну інформацією між сторонами призводить до того, що А шифрує повідомлення ключем $К_{АВ}$ та надсилає його. Зловмисник перехоплює цього листа, розшифровує його перехопленим ключем сторони А($К_{АВ}$), перешифровує ключем, який він надіслав В ($К_{ЗВ}$) та відправляє. Сторона В, отримавши зашифрованого листа, розшифровує його і, оскільки сеанс розшифрування пройшов успішно, «вірить», що обмін інформацією триває нормально. При спробі сторони В відповісти на лист від А, зловмисник виконує аналогічну процедуру.

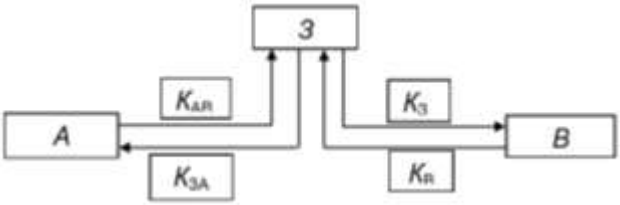

Рисунок 4.3 – Схема атаки Man-in-Middle під час обміну криптографічними ключами

Таким чином, зловмисник читає усю інформацію, що курсує між сторонами А та В, оскільки володіє усіма чотирма криптографічними ключами, а продовжуватися це може доти, допоки сторони А та В не зустрінуться фізично та не зрозуміють, що оперують незнайомими криптографічними ключами, або З не використає проти них перехоплену інформацію.

Посередництво – одна з найнебезпечніших атак проти систем зв'язку. Захист від нього потребував створення потужної системи – інфраструктури відкритих ключів та застосування геш-функцій. Успішний захист від посередництва полягає у обчисленні геш-образу повідомлень та підписуванні цього образу електронним цифровим підписом. У такому разі отримувач має змогу перевірити цілісність інформації порівнянням геш-функцій та власника цифрового підпису за допомогою сертифіката інфраструктури відкритих ключів (PKI).

Нижче наведено приклад специфічного типу атак на криптосистему RSA.

1. Атака на близькі значення p і q. Однією із найвідоміших атак на криптосистему RSA є така, що використовує близькі значення p та q. Припустимо, що p>q, хоча це ніяк не обмежує подальші припущення. Тоді можна записати:

$$x=(p+q)/2;\ y=(p-q)/2,$$

а для n справедливим буде наступне рівняння:

$$n=x2-y2.$$

Для знаходження множників p та q досить підібрати числа x та y, що задовольняють (*). Знайдемо $x_0 = \sqrt{n}$ та оберемо найближче до нього більше ціле x1. Підставляючи його у (*), знаходимо відповідне значення y. Повторюємо цю операцію доти, поки не отримаємо цілі значення x та y, що задовольняють (*).

У результаті знаходимо: p=x+y, q=x−y.

2. Атака з вибраним шифротекстом. Нехай перехоплено повідомлення $C=E^e(M)$, зашифроване на публічному ключі алгоритму RSA.

Обираємо число $r<n$, та обчислюємо:

$$x=r^e \bmod n;\ y=x^C \bmod n;$$

$$t=r^{-1} \bmod n.$$

Якщо $x=r^e \bmod n$, тоді $r=x^d \bmod n$.

Тепер просимо власника ключа підписати у приватним ключем d. Будемо мати $u=y^d \bmod n$.

Обчислимо $t^u \bmod n=r^{-1}y^d \bmod n=r^{-1}x^dC^d \bmod {}^n=C^d \bmod n=M$. Таким чином, отримано розшифроване повідомлення M.

Захист від такої атаки може здійснюватися двома шляхами. Перший полягає в тому, що пари ключів для шифрування та електронного підпису повинні бути різними. Другий – підписувати завжди потрібно геш-образ повідомлення, а не власне повідомлення.

3. Атака на електронний підпис. Якщо зловмиснику необхідно отримати електронний підпис повідомлення M, він може діяти таким чином. Створюються повідомлення M_1 та M_2 такі, що $M=M_1M_2 \bmod n$, та підписуються окремо повідомлення M_1 та M_2. Якщо є електронний цифровий підпис (ЕЦП) повідомлень M_1 та M_2, тоді:

$$M_3^d=(M_1^d \bmod n)\times(M_2^d \bmod n),$$

а отже, повідомлення M підписано.

4. Атака на спільний модуль. При реалізації RSA іноді буває вигідним роздати усім користувачам спільний модуль n та різні ключі e та d. Однак така схема працює доти, доки два користувача не зашифрують на різних ключах однакове повідомлення. Якщо e_1 та e_2 – взаємно прості числа, тоді можлива така атака.

Нехай m – повідомлення, e_1 та e_2 – два публічних ключа, n – спільний модуль. Процес шифрування можна зобразити наступним рівняннями:

$$C_1=m^{e_1} \bmod n;\ C_2=m^{e_2} \bmod n.$$

Отже, криптоаналітик знає n, e_1, e_2, C_1, C_2. За допомогою алгоритму Евкліда він знаходить такі r та s, які задовольняють рівняння:

$$s^{e_1}+r^{e_2}=1 (r<0;\ s>0)$$ та обчислює C_1-1 mod n.

Тоді $(C_1^{-1})^{-r}C_2^s \bmod n=m$.

Доведемо це, підставивши замість C_1 та C_2 їх значення:

$$((m^{e_1})^{-1})^r m^{e_2 s} \bmod n=m^{e_1 r}m^{e_2 s} \bmod n=m^{e_1 r+e_2 s} \bmod n=m.$$

Зважаючи на таку атаку, задавати спільний модуль для групи користувачів є дуже небезпечним.

5. Атака дешифрування ітераціями. Суть методу полягає в тому, що перехоплену криптограму повторно шифрують на публічному ключі і при деякій кількості ітерацій отримують вихідне повідомлення. Кількість ітерацій, звичайно, залежить від довжини модуля та ключа. За невеликої довжини модуля цього можна досягти вже при кількох ітераціях.

4.4 Механізми захисту від атак

Багатошаровий захист – це стратегія безпеки, в якій кілька захисних шарів розміщено через усю інформаційну систему. Це допомагає уникнути прямих атак проти інформаційної системи і даних, оскільки злом одного шару призводить зловмисника лише до наступного рівня.

Управління інцидентами – це набір певних процесів для ідентифікації, аналізу, присвоювання пріоритетів і рішення інцидентів безпеки для відновлення нормальних сервісних операцій так швидко, як це можливо і уникнення майбутнього повторення інциденту.

Політика безпеки – це документ або набір документів, який описує управління безпекою, яке буде реалізовано в організації.

Процес дослідження вразливостей і помилок проєктування, який відкриває операційну систему та її застосування для атаки або зловживання.

Тестування на проникнення – це метод оцінювання інформаційної безпеки системи або мережі симуляцією атаки для пошуку вразливостей, які може використовувати зловмисник. Тестування містить активний аналіз конфігурації системи, пошук недоліків проєктування, архітектури мережі, технічних недоліків і вразливостей

4.5 Диференціальний криптоаналіз

Поняття диференціального криптоаналізу було введено Елі Біхамом (A. Biham) та Аді Шаміром (A. Shamir) у 1990 році. Диференціальний криптоаналіз використовують для атак на симетричні криптосистеми. Кінцеве завдання диференціального криптоаналізу – використовуючи властивості алгоритму, в основному властивості S-блоків, визначити підключ раунду. Конкретний спосіб диференціального криптоаналізу залежить від алгоритму шифрування.

Якщо в основі алгоритму лежить сітка Фейстеля, то можна вважати, що блок m складається з двох половинок – m_0 і m_1. Диференціальний криптоаналіз розглядає відмінності, які відбуваються в кожній половині при шифруванні (наприклад, для алгоритму DES «відмінності» визначаються за допомогою операції XOR, для інших алгоритмів можливий інший спосіб). Обирається пара

незашифрованих текстів з фіксованою відмінністю. Потім аналізуються відмінності, що вийшли після шифрування одним раундом алгоритму, і визначаються ймовірності різних ключів. Якщо для багатьох пар вхідних значень, що мають ту саму відмінність X, при використанні того самого підключа Y однаковими виявляються і відмінності відповідних вихідних значень, то можна припустити, що в X використано підключ Y з певною ймовірністю. Якщо ця ймовірність близька до одиниці, то можна вважати, що підключ раунду знайдений з даною ймовірністю. Імовірність знаходження загального ключа визначається добутком ймовірностей підключів кожного раунду, оскільки раунди незалежні.

Результати диференціального криптоаналізу використовуються для розроблення конкретних S-блоків та визначення оптимальної кількості раундів.

Диференціальний криптоаналіз на основі відмов пристрою. У вересні 1996 року група фахівців із компанії Bellcore оголосила про новий метод криптоаналізу, що дозволяє ефективно розкривати секретний ключ, який зберігається в пам'яті портативного шифрувального обладнання (наприклад, Smart Card або PCMCIA). Збереження ключа в таких пристроях забезпечується за рахунок унікальних характеристик технології TEMPEST. Вперше метод був успішно застосований для розкриття ключа криптосистеми RSA. Подальші дослідження нового методу, що одержав назву диференціального криптоаналізу на основі відмов обладнання (DFA – Differential Fault Analysis), продемонстрували його ефективність при атаці на DES й інші блокові шифри. Так, для розкриття ключа DES знадобилося проаналізувати двісті шифротекстів, отриманих шифруванням відкритих текстів, які зберігаються в пам'яті обладнання. Було доведено, що навіть застосування потрійного DES не впливає на складність атаки.

Відомо, що деякі види випромінювання (наприклад, радіоактивне) призводять до відмов електронного устаткування. Саме ця ідея і лягла в основу крипоаналітичної атаки, розробленої криптоаналітиками компанії Bellcore. При цьому передбачається, що криптоаналітик має необмежений доступ до шифрувального обладнання. Відкритий текст і секретний ключ зберігаються в пам'яті обладнання і недоступні. Криптоаналітик штучно викликає відмови в роботі обладнання, піддаючи його опроміненню. Опромінення призводить до інверсії біта (або бітів) в одному з регістрів на деякому проміжному етапі криптографічного перетворення (наприклад, для блокових шифрів конструкції Фейстеля інверсія виникає на одному із циклів перетворення). Відмова призводить до спотворення шифротексту на виході обладнання. Криптоаналітик

намагається розкрити секретний ключ, аналізуючи спотворені і неспотворені шифротексти.

Розглянемо описаний метод на прикладі криптоаналізу DES. Припустимо, що є два різні шифротексти, отримані при шифруванні того самого відкритого тексту на фіксованому ключі. Відомо, який шифротекст отриманий у результаті інверсії одиночного біта в процесі шифрування. На першому етапі атаки необхідно встановити номер циклу перетворення, на якому відбулась інверсія. Припустимо, що інверсія відбулася на останньому, шістнадцятому циклі DES-перетворення в правій половині блоку до заключної перестановки. Звідси зрозуміло, що відмінність лівих половин блоків шифротексту визначається виходами тих S-блоків (одного або двох), на вході яких з'явився інвертований біт. Застосування методу диференціального криптоаналізу дозволяє розкрити шість бітів ключа для кожного такого S-блоку.

Для розкриття підключа останнього циклу перетворення досить проаналізувати менше 200 шифротекстів. Подальший розвиток атаки можливий у двох напрямах. Перший варіант – пошук секретного ключа шляхом вичерпної перевірки 28=256 кандидатів при заданому підключі (нагадаємо, що розрядність підключа – 48 бітів). Альтернативний варіант полягає у використанні знання про підключ, отриманий на останньому циклі для аналізу попередніх циклів. Останній варіант дозволяє успішно атакувати DES у режимі EDE-шифрування на трьох різних ключах. Описаний метод працює й у тих випадках, коли інверсія виникає всередині F-функції або процедури генерації підключів.

Метод диференціального криптоаналізу на основі відмов обладнання можна застосовувати для атаки на такі блокові шифри, як IDEA, RC5 і Feal. Деякі блокові шифри, наприклад, Khufu, Khafre і Blowfish використовують заданий секретний ключ для генерації S-блоків. У цьому випадку описаний метод дозволяє розкривати не тільки ключі, але й власне S-блоки.

Розглянутий криптоаналітичний метод дозволяє ефективно розкривати ключ шифрування навіть тоді, коли сам алгоритм криптографічного перетворення невідомий. Так, наприклад, деталі криптоалгоритму Fortezza становлять державну таємницю і засекречені Агентством національної безпеки США. Однак апаратна реалізація криптоалгоритму у вигляді мікросхеми Clipper входить до складу багатьох комерційних обладнань шифрування. Більше того, можливе відновлення деталей невідомого алгоритму.

4.6 Лінійний криптоаналіз

Метод лінійного криптоаналізу вперше було застосовано для атаки

блокового шифру FEAL, а пізніше DES. Метод використовує лінійні наближення. Це означає, що якщо виконати операцію XOR над деякими бітами відкритого тексту, потім над деякими бітами шифротексту, а потім виконати XOR результатів попереднього сумування, можна одержати біт, який буде сумою кількох бітів ключа. Це і є лінійним наближенням, яке може бути правильним з деякою ймовірністю p. Якщо $p \neq 1/2$, то цей факт можна використовувати для розкриття бітів ключа.

У загальному вигляді лінійний криптоаналіз матиме вигляд:

$$\sum_{i=1}^{a} P_i \oplus \sum_{j=1}^{b} C_j = \sum_{l=1}^{c} K_l,$$

де $i_1, i_2, ..., i_a$; $j_1, j_2, ..., j_b$ та $l_1, l_2, \ldots, l_c$ – позиції деяких бітів відкритого тексту Pi, шифротексту Cj ключа Kl.

Успіх лінійного криптоаналізу не аби як залежить від структури S-блоків і виявилося, що S-блоки DES не оптимізовано проти такого способу розкриття. Стверджують, що стійкість до лінійного криптоаналізу не входила у число критеріїв при проектуванні DES. Причина цього невідома: або розробники не знали про можливості лінійного криптоаналізу, або віддали перевагу стійкості проти диференціального, найбільш небезпечного з їхньої точки зору методу.

Підраховано, що для найкращого лінійного наближення необхідно 247 відомих відкритих блоків, а результатом буде 1 біт ключа. Це дуже мало. Якщо змінити напрям і використовувати для аналізу шифротекст, а не відкритий текст, а також розшифрування замість шифрування, то в результаті лінійного криптоаналізу можна отримати 2 біти ключа. Це все ще недостатньо.

Однак існують деякі тонкощі. Якщо використати лінійний криптоаналіз паралельно 212 разів та обрати правильний варіант, ґрунтуючись на ймовірностях, це дасть 12 бітів ключа. 13 бітів ключа можна отримати, змінивши шифрування на розшифрування, а інших 30 біт – «грубою силою», тобто повним перебиранням.

Розкриття повного 16-раундового DES за такою схемою вимагає 243 відомих відкритих текстів. Програмна реалізація цього методу на 12 робочих станціях HP9735, розкрила ключ DES за 50 днів. Лінійний криптоаналіз молодший за диференціальний, тому дуже імовірний подальший розвиток цих ідей.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Загроза інформаційної безпеки.

2. Класифікація загроз інформаційної безпеки автоматизованих систем.
3. Типи атак на інформаційні системи.
4. Класифікація атак на симетричні та асиметричні криптоалгоритми.
5. Типи загроз інформаційного обміну.
6. Основні типи атак в симетричних криптоалгоритмах.
7. Механізми захисту від атак.
8. Багатошаровий захист та управління інцидентами.
9. Диференціальний та лінійний криптоаналіз.
10. У чому полягає суть атаки «chosen-text attack»?
11. У чому полягає суть атаки «chosen-ciphertext attack»?
12. У чому полягає суть атак на спільний модуль, електронний підпис та дешифрування ітераціями?

Література: [2; 5-11; 14-17].

Тема 5. Механізми і політики розмежування прав доступу

План:
5.1 TCSEC
5.2 Common Criteria
5.3 НД ТЗІ 2.5-004-99

5.1 TCSEC

Стандарт Міністерства оборони США TCSEC, більш відомий як «Оранжева книга» за кольором обкладинки, був затверджений у 1983 році та оновлений у 1985. Повна назва документа – «Department of Defense Trusted Computer System Evaluation Criteria» – Критерії оцінки захищених комп'ютерних систем Міністерства оборони. Це був перший стандарт, який встановлював основні вимоги до оцінки ефективності засобів безпеки комп'ютерних систем. З цієї точки зору його значення важко переоцінити, оскільки з'явився загальновизнаний базис понять, без якого навіть обговорення проблем інформаційної безпеки було б складним завданням.

Необхідно зупинитися на відмінностях між термінами «захищена система», яке використовують в Україні, і «довірена система», яке використовують в англомовній літературі. «Оранжева книга» (ОК) була першим документом, де стверджувалося, що будь-яких абсолютних систем (у тому числі й абсолютно безпечних) у нашому житті не існує. Тому було запропоновано оцінювати лише степінь довіри до цієї чи іншої системи, тобто наскільки можна їй довіряти. В

українській літературі оцінюють не степінь довіри, а степінь захищеності КС.

ОК дала визначення поняттю безпечної системи. Згідно з нею, безпечною комп'ютерною системою називається така, де тільки уповноважені користувачі або процеси від їх імені можуть читати та змінювати призначену для них інформацію. Це означає, що доступ до інформації повинні мати лише уповноважені користувачі, причому вони повинні мати доступ не до всієї інформації, а лише до призначеної для них.

Основні термінологія «Оранжевої книги». ОК зуміла виробити так звані принципи безпеки, які наведено нижче.

1. Безпечні системи повинні керуватися розробленими політиками безпеки, а користувачі зобов'язані їх дотримуватися.

2. Кожен об'єкт безпечної системи повинен мати певний рівень безпеки (рівень доступу для користувачів, рівень безпеки – для інформації), який визначається так званими мітками безпеки.

3. Обов'язковою складовою безпечної системи повинна бути автентифікація користувачів.

4. У безпечних системах повинен бути налагоджений аудит за усіма важливими подіями, що відбуваються в системі і мають відношення до безпеки (журнали аудиту повинні бути захищеними від зміни).

5. Засоби захисту безпечних систем повинні знаходитися під постійним контролем деякої системи, що контролює правильність їх роботи.

6. Принцип неперервності захисту: не повинно бути моментів у роботі системи, коли засоби захисту неактивні.

Проаналізуємо кожен із цих принципів безпеки, звернувши увагу на те, що пропонує ОК для того, щоб захищена система задовольняла ці принципи безпеки.

1. Політики безпеки. Політики безпеки повинні бути детальними, чітко визначеними та обов'язковими для виконання усіма користувачами комп'ютерної системи. ОК пропонує два типи політики безпеки: мандатна політика – така, яка ґрунтується на порівнянні внутрішніми засобами системи рівнів доступу користувачів та рівнів секретності інформації (усі рівні задаються так званими мітками безпеки) і прийнятті рішення про допуск до інформації; дискреційна політика – така, коли прийняття рішення про допуск до інформації ґрунтується на зовнішніх щодо системи захисту правилах доступу.

2. Мітки безпеки. ОК вважає, і це стало вже стандартом інформаційної безпеки, що мандатна політика безпеки безпечніша за дискреційну, що, як

можна спостерігати пізніше, відображено в класах безпеки.

3. Відповідальність. Незалежно від обраної політики безпеки, повинна існувати індивідуальна відповідальність користувачів за усі дії в системі. ОК висуває три вимоги до відповідальності:

– автентифікація – процес, який надає підтвердження про те, що користувач є саме тим, ким він представився системі;

– авторизація – надання користувачеві певних повноважень у системі;

– аудит – здатність системи контролювати усі важливі дії користувачів у захищених журналах аудиту.

4. Монітор звернень. Контроль за виконанням користувачами обробки інформації повинен вестися за допомогою деякої системи, яку ОК називає монітором звернень, яка має задовольняти таким умовам:

– ізольованість, тобто неможливість відстеження його роботи;

– повнота, тобто неможливість обійти монітор;

– верифікованість, тобто можливість аналізу та тестування.

5. Ядро безпеки – це певна реалізація монітора звернень з гарантованим рівнем безпеки.

6. Гарантії безпеки. Взагалі ОК приділяє значну увагу рівню гарантованості безпеки. Вважається, що комп'ютерна система повинна містити апаратні та/або програмні механізми, які повинні незалежно підтверджувати впевненість в тому, що система має задекларований рівень захищеності, а підсистема безпеки працює тільки так, як заплановано. Для досягнення цієї мети необхідно два типи гарантій:

– операційна гарантія – впевненість в тому, що реалізація спроектованої системи забезпечує правильне втілення розробленої системи захисту;

– гарантія життєвого циклу – впевненість в тому, що розробка та підтримка системи виконані відповідно до формалізованих та жорстко контрольованих критеріїв функціонування; сюди відносяться: аудит спроектованої системи безпеки, технічного завдання, способів керування налаштуваннями та відповідності реальних параметрів тим, які були заявлені;

– гарантії неперервності захисту – надійні механізми, які забезпечують неперервний захист основних засобів від несанкціонованих змін.

7. До гарантій неперервності захисту можна ще додати те, що система повинна бути спроектована таким чином, щоби користувачі не допускалися до обробки інформації не через систему захисту. Простіше кажучи, при завантаженні системи спочатку стартує підсистема захисту, а потім, коли служби захисту активні, – вже допускаються користувачі.

Згідно з таким уявленнями про безпечні та довірені системи, в ОК було розроблено вимоги для захищених систем.

5.2 Common Criteria

Цей стандарт було розроблено у 1999 році, причому відчувається великий вплив Оранжевої книги. Стандарт ISO/IES 15408, повна назва якого «Evaluation criteria for IT security» (Критерії оцінки безпеки інформаційних технологій) отримав назву «Загальні критерії» (ЗК).

Сьогодні «Загальні критерії» – це найбільш повний та сучасний стандарт оцінювання. Насправді – це метастандарт, який визначає інструменти оцінки безпеки інформаційних систем і порядок їх використання. ЗК містять два основних типи вимог безпеки:

– функціональні, які ставляться до функцій безпеки та механізмів, що їх реалізують;

– вимоги довіри, які ставляться до технології та процесу розробки і експлуатації.

Функціональні вимоги згруповані на основі ролі, яку вони виконують або засобу безпеки, який вони обслуговують. Усього є 11 функціональних класів, розбитих на три групи, 66 сімейств, 135 компонентів.

Перша група визначає елементарні сервіси безпеки:

– FAU – вимоги до сервісу аудиту;

– FIA – вимоги до ідентифікації та автентифікації;

– FRU – вимоги до використання ресурсів.

Друга група визначає сервіси, похідні від елементарних:

– FCO – вимоги до безпеки комунікацій учасників інформаційного обміну;

– FPR – вимоги до приватності;

– FDP – вимоги до захисту даних користувача;

– FPT – вимоги до захисту функцій безпеки самої підсистеми захисту.

Третя група пов’язана з інфраструктурою системи:

– FCS – вимоги до криптографічної підтримки (обслуговування керування ключами та операцій шифрування/розшифрування);

– FMT – вимоги до керування засобами безпеки;

– FTA – вимоги до керування доступом;

– FTP – вимоги до довіреного каналу.

Вимоги довіри (гарантій безпеки) – вимоги, що ставляться до технологій та процесу розробки та експлуатації об’єкта. Ці вимоги розділено на 10 класів, 44

сімейства та 93 компонента. Усі десять класів розбиті на дві групи.

Перша група містить класи вимог, які передують розробці та оцінці об'єктів:

– APE – вимоги до оцінки профілю захисту;
– ASE – вимоги до оцінки завдання безпеки.

Друга група пов'язана з етапами життєвого циклу об'єкта, що розглядається:

– ADV – вимоги до розробки, проектування об'єкта;
– ALC – вимоги до підтримки життєвого циклу;
– ACM – вимоги до керування конфігурацією;
– AGD – вимоги до посібника користувача та адміністратора;
– ATE – вимоги до тестування;
– AVA – вимоги до оцінки вразливостей;
– ADO – вимоги до постачанню та експлуатації;
– AMA – вимоги до підтримки довіри після сертифікації об'єкта.

Функціональні вимоги безпеки. Нагадаємо, що у цьому розділі містяться три класи функціональних вимог безпеки:

– FAU – аудит, тобто вимоги до сервісу аудиту;
– FIA – вимоги до ідентифікації та автентифікації;
– FRU – вимоги до використання ресурсів.

Клас FAU складається з шести сімейств (FAU_GEN, FAU_SEL, FAU_STG, FAU_SAR, FAU_SAA), користуючись якими можна сформулювати вимоги до відбору, реєстрування, збереження та аналізу даних про події, що мають відношення до інформаційної безпеки.

Сімейство FAU_GEN описує генерування даних для аудиту. Ця система включає два компоненти, FAU_GEN.1 та FAU_GEN.2. Система, яка задовольняє клас FAU_GEN.1, повинна вести журнал аудиту з мінімальним набором даних (дату, час, тип та результат події, ідентифікатор суб'єкта). Система класу FAU_GEN.2 окрім цього ще повинна в обов'язковому порядку асоціювати кожну подію з ідентифікатором користувача, що його ініціював.

Сімейство FAU_SEL визначає вимоги до засобів відбору подій для аудиту. Відбір може відбуватися на основі таких атрибутів, як ідентифікатори об'єктів або суб'єктів, ідентифікатора користувача, вузла мережі, тип події тощо. Також передбачається визначення додаткових атрибутів.

Сімейство FAU_STG визначає вимоги до зберігання даних аудиту. Воно містить дві пари компонентів: FAU_STG.1 та FAU_STG.2; FAU_STG.4 та FAU_STG.5. FAU_STG.1 визначає вимоги до захисту даних журналів аудиту;

FAU_STG.2 – гарантії доступності журналів аудиту для адміністраторів. Друга пара визначає дії системи у випадку можливої втрати даних аудиту. Згідно з FAU_STG.4 і FAU_STG.5 система може ігнорувати та заборонити події без аудиту, записати нові дані, знищивши найстарші тощо.

Сімейство FAU_SAR визначає права на повне або часткове читання (на основі критеріїв з логічними функціями) журналів реєстраційної інформації уповноваженими користувачами та заборона доступу до них для решти користувачів.

Сімейство FAU_SAA встановлює вимоги до засобів автоматичного аналізу функціонування системи, які дозволяють з'ясувати можливі порушення безпеки. Це сімейство також складається з чотирьох компонентів. Базовий компонент сімейства, FAU_SAA.1 регламентує застосування набору правил накопичення або об'єднання подій, які сигналізують про імовірне порушення політики безпеки. FAU_SAA.2 підсилює FAU_SAA.1, він уводить поняття профілю поведінки, рейтингу підозрілої активності для кожного користувача, а також порогу, перевищення якого вказує на імовірне порушення політики безпеки. FAU_SAA.3 та FAU_SAA.4 визначають поняття сигнатури атаки різних ступенів складності та функції виявлення сигнатур у реальному масштабі часу. Разом вони визначають просту та складну евристику атаки.

Шосте сімейство, FAU_ARP (автоматична реакція аудиту безпеки), визначає дії, які необхідно виконати системі після виявлення імовірних порушень безпеки. Таким чином, ЗК вперше застосовують методи активного аудиту.

Шість сімейств класу FIA містять вимоги до ідентифікації та автентифікації користувачів та до пов'язування атрибутів безпеки з ідентифікаторами користувачів.

Сімейство FIA_UID відповідає за ідентифікацію користувачів, складається з двох компонентів та визначає набір дій, які дозволено виконувати до ідентифікації. Наприклад, такою дією може бути отримання довідкової інформації. Однак більш сильний компонент, а саме FIA_UID.2, не дозволяє ніяких дій до виконання ідентифікації.

Сімейство FIA_UAU (автентифікація користувача) специфікує механізми автентифікації та її атрибути. Компоненти FIA_UAU.1 (вибір моменту автентифікації) та FIA_UAU.2 (автентифікація до будь-яких дій користувача) спрямовані на безпеку простої автентифікації, а FIA_UAU.3 (захищена від підробок автентифікація) та FIA_UAU.4 (механізми одноразової автентифікації) – на реалізацію надійної автентифікації, стійкої до мережевих атак. Якщо

потрібна ще сильніша автентифікація, використовують FIA_UAU.5 (використання кількох механізмів автентифікації), FIA_UAU.6 (повторна автентифікація) та FIA_UAU.7 (автентифікація із захищеним зворотним зв'язком).

Сімейство FIA_ATD (визначення атрибутів користувача) передбачає наявність у користувачів не тільки ідентифікаторів, але й інших атрибутів безпеки, які визначаються політикою безпеки.

Сімейство FIA_USB описує вимоги до зв'язування атрибутів безпеки користувача з суб'єктом доступу, тобто процесом, який діє в системі від імені цього користувача. Виявленням та реагуванням на невдалі спроби автентифікації займається сімейство FIA_AFL (відмови автентифікації). Це означає, що воно визначає дії системи при невдалій автентифікації, а також кількість дозволених спроб автентифікації. Сімейство складається з одного компонента.

Сімейство FIA_SOS специфікує метрику якості інформації, яку сповіщає системі користувач під час автентифікації та вимоги до засобів перевірки цієї якості, наприклад, технічних обмежень на паролі користувачів або програмних генераторів паролів.

Клас FRU (використання ресурсів) складається з трьох сімейств, які призначені підтримувати високий степінь доступності інформації.

Виконання вимог сімейства FRU_FLT (стійкість до відмов) повинно забезпечити коректну роботу усіх або деяких функцій системи навіть у випадку відмов.

Сімейство FRU_PRS (пріоритет обслуговування) регламентує дії із захисту операцій високого пріоритету з боку операцій з нижчим пріоритетом.

Сімейство FRU_RSA (розподіл ресурсів) визначає квоти для досягнення високої доступності ресурсів. Однією з переваг ЗК є увага до доступності ресурсів, однак тут не спостерігається системного підходу, оскільки доступність можна підтримувати й іншими механізмами, наприклад, балансування навантаження, проактивне керування, використання багатопроцесорних конфігурацій, організація резервних обчислювальних систем тощо. Ці питання зовсім не розглядаються у ЗК.

Вимоги довіри (гарантії безпеки). Вимоги довіри – це сукупність вимог, що висуваються до технологій та процесів розробки проектів безпеки, а також до експлуатації захищених систем. Дотримання цих вимог допомагає з'ясувати, наскільки якісним буде проект захисту, чи не матиме він протиріч тощо. Ці вимоги розділено на десять класів та 44 сімейства.

Вимоги класу APE (оцінка профілю захисту) та ASE (оцінка завдання

безпеки) зосереджуються на перевірці повноти та можливості реалізації бажаного проекту безпеки. Клас APE складається з шести однокомпонентних сімейств, що відповідають структурі профілів захисту.

Сімейство APE_INT висуває вимоги до анотації та вступу до проекту безпеки. Спеціаліст повинен підтвердити, що зібрана інформація не протирічить іншим частинам проекту безпеки. Такі дії стандартні при будь-яких оцінках захищених систем.

Сімейство APE_DES визначає правила опису об'єктів, для яких проектується (або оцінюється) система безпеки. Такий опис повинен, як мінімум, тип та загальну характеристику системи.

Вимоги сімейства APE_ENV зосереджені на аналізі середовища, в якому буде функціонувати (або вже функціонує) система безпеки. Тут необхідно описати усі актуальні загрози, усі обов'язкові для виконання політики безпеки.

Сімейство APE_OBJ висуває вимоги до формування цілей безпеки для системи та її середовища, їх обґрунтування.

Основний зміст профілю захисту складають вимоги безпеки. Ці вимоги формулюються в класах APE_REQ та APE_SRE. Логічне обґрунтування вимог безпеки повинно продемонструвати їх вирішальну роль у досягненні цілей безпеки.

Клас ASE влаштований аналогічно до APE, однак деякі відмінності викликані більшою конкретністю завдання з безпеки порівняно з профілем захисту та наявністю додаткових розділів. Також модифіковано вимоги шести попередніх сімейств та додано два нових.

Дотримання вимог описаних класів дуже важливе, оскільки проблеми на стадії проектування та специфікації обчислювальних систем може призвести до тяжких наслідків на стадії експлуатації, виправити які може бути надзвичайно важко та дорого.

Вимоги довіри до етапу розробки. Функціональні вимоги, політика безпеки та специфікація системи є основою для розробки функцій безпеки.

Клас ADV (розробка) складається з семи багатокомпонентних сімейств і містить вимоги для поступового підвищення рівня деталізації проекту аж до реалізації з демонструванням відповідності заданим рівням. У цьому класі передбачено три стилі специфікацій: неформальний, напівформальний і формальний та три способи демонстрації відповідності.

Неформальну специфікацію пишуть як звичайний текст з визначенням необхідних термінів.

Напівформальна специфікація складається за допомогою мови з обмеженим

синтаксисом, формальна – використовує математичну нотацію та вимагає формального доведення.

Технологічні вимоги процедурного характеру складають зміст класу ALC (підтримка життєвого циклу). Він складається з чотирьох сімейств: ALC_LCD (вимоги до моделей життєвого циклу); ALC_TAT (обґрунтування вибору інструментальних засобів та методів); ALC_DVS (вимоги до безпеки розробки); ALC_FLR (вимоги до усунення недоліків).

Клас ACM (управління конфігурацією) містить три сімейства: ACM_CAP (специфікація можливостей управління конфігурацією); ACM_SCP (представлення реалізації об'єкта); ACM_AUT (автоматизація управління конфігурації).

Вимоги довіри до етапу отримання, подання та аналізу результатів розробки. Ці вимоги складаються з трьох класів: AGD (вимоги до посібників користувача); ATE (вимоги до тестування); AVA (оцінка вразливостей).

Клас AGD складається з двох однокомпонентних сімейств, де сформульовано вимоги до посібників адміністратора (AGD_ADM) та користувача (AGD_USR).

Клас ATE висуває вимоги до тестування та складається з чотирьох сімейств: ATE_FUN (вимоги до функціонального тестування); ATE_DPT (вимоги до обґрунтування достатньої глибини); ATE_COV (вимоги до обґрунтування достатнього покриття).

Функціональне тестування виконує розробник. При функціональному тестуванні необхідно перевірити усі функції безпеки, звертаючи також увагу на відсутність небажаних (нерегламентованих) режимів функціонування. Аналіз глибини тестування повинен підтвердити достатність розроблених тестів для демонстрування того, що функції безпеки виконуються відповідно до розроблених проектів. Аналіз покриття повинен продемонструвати повну відповідність функціональній специфікації. При такому аналізі необхідно повність перекрити всі зовнішні інтерфейси функцій безпеки.

Сімейство ATE_IND (вимоги до незалежного тестування) регламентує дії тестувальників. Їм необхідно протестувати необхідну підмножину функцій безпеки та підтвердити, що система працює відповідно до специфікацій. Також треба виконати деякі (або навіть усі) тести з тестової документації, щоби підтвердити результати виробника.

Вимоги до оцінки вразливостей висуває клас AVA. Основою для нього служить аналіз вразливостей (сімейство AVA_VLA), який виконується і розробником, і аналітиком. Це сімейство має чотири компоненти, які

підвищують вимоги: AVA_VLA.1 та AVA_VLA.2 висувають вимоги до низького потенціалу порушника; AVA_VLA.3 (середній потенціал порушника), AVA_VLA.4 – високого потенціалу.

Вимоги до аналізу стійкості функцій безпеки системи висуваються сімейством AVA_SOF і виконується на рівні механізмів. Це означає, що для кожного механізму необхідно показати, що його стійкість досягла або перевищила рівень, заданий у профілі захисту або проекті безпеки.

Вимоги сімейства AVA_MSU (неправильне застосування) спрямовані на те, щоб виключити можливість такого конфігурування або застосування системи, які є небезпечними в той час, коли адміністратор або користувач вважають їх абсолютно безпечними. Для того, щоб виключити таку можливість, необхідно забезпечити повну однозначність вказівок посібників, проаналізувати їх текст на наявність необґрунтованих, протирічивих процедур. Небезпечні стани повинні легко виявлятися. Аналітики повинні повторити усі процедури конфігурування та інсталяції системи, інші процедури для підтвердження того факту, що систему можна безпечно конфігурувати та використовувати, використовуючи лише надані посібники. Крім цього, вони повинні виконати незалежне тестування та перевірити, чи зможуть адміністратор та користувач за допомогою посібника з'ясувати, що система відконфігурована або використовується небезпечним чином.

Аналіз прихованих каналів, який регламентується сімейством AVA_CCA, досить складний. Розробник повинен провести вичерпний пошук прихованих каналів для кожної політики керування інформаційними потоками та надає документацію для аналізу, де ідентифіковано приховані канали та проведено оцінку їхньої пропускної здатності, описано найбільш небезпечні варіанти використання кожного прихованого каналу. Аналітик повинен вибірково підтвердити правильність зробленого виробником аналізу прихованих каналів засобами незалежного тестування.

Вимоги до постачання та експлуатації, підтримка довіри. Вимоги до постачання та експлуатації визначаються класом ADO, який складається з двох сімейств: трикомпонентного ADO_DEL (вимоги до постачання), ADO_IGS (вимоги до встановлення, генерування та запуску). Цей клас висуває вимоги до документації та процедур, які здатні виявити відмінності поставленого продукту від оригіналу, а також спроб підміни від імені розробника, якщо останній нічого не постачав. Щодо процедур встановлення та запуску, то процедури безпечного виконання цих операцій також мають бути однозначно визначені та описані в посібниках адміністратора та користувача.

Клас AMA (вимоги до підтримки довіри) складається з чотирьох сімейств та містить вимоги, які будуть корисні після сертифікації системи. Вони допомагають зберегти впевненість у тому, що система продовжує відповідати заданим вимогам безпеки після того, як з часом відбулися зміни у ній самій або у оточуючому середовищі. Тут мова йде про появу нових загроз або вразливостей, зміну вимог користувача або виправлення помилок.

Дії з підтримки довіри мають циклічний характер. Кожна ітерація циклу складається з двох фаз: приймання системи для підтримки та моніторингу системи. Фаза приймання включає розробку планів підтримки довіри та категоріювання компонентів системи за їх впливом на безпеку. Елементи фази моніторингу – подання опису поточної версії системи та виконання аналізу впливу змін на рівень безпеки. Можливо, наприкінці ітерації виявиться, що план або категорія системи вимагають уточнення або зміни; тоді нова ітерація почнеться з повторного приймання системи.

Однак цикл підтримки довіри не може тривати безмежно. Рано чи пізно в системі накопичиться багато мілких змін та недоліків, виникнуть серйозні проблеми, які вимагатимуть повторного оцінювання системи.

Рівні оцінки довіри «Загальних критеріїв». «Загальні критерії» визначили сім впорядкованих рівнів оцінки довіри безпеки. Ці рівні містять комбінації вимог довіри, розраховані на довгострокове застосування. Така шкала надає можливість збалансувати отриманий рівень довіри з термінами, складністю, вартістю розробки.

Перший рівень довіри передбачає функціональне тестування та може застосовуватися тоді, коли вимагається деяка впевненість, що система захисту працює бездоганно, а загрози не вважаються серйозними. Його можна досягнути з мінімальними витратами без допомоги розробників аналізом функціональних специфікацій, специфікації інтерфейсів, експлуатаційної документації разом з незалежним тестуванням.

Другий рівень довіри передбачає структурне тестування і доступ до частини проектної документації та результатам тестування розробником. Цей рівень застосовують тоді, коли розробнику або замовнику необхідно отримати середній рівень довіри при відсутності доступу в повному обсязі до документації розробника.

На додаток до Першого рівня, тут необхідний аналіз проекту верхнього рівня. Аналіз повинен підтримуватися незалежним тестуванням функцій безпеки, актом розробника про випробування функціональних специфікацій, вибірковими незалежними підтвердженнями результатів тестування; аналізом

стійкості функцій та свідоцтвом пошуку явних вразливостей. Також необхідний перелік конфігурації системи з унікальною ідентифікацією її елементів та свідоцтва безпечних процедур постачання.

Третій рівень довіри передбачає систематичне тестування та перевірку функцій безпеки і дозволяє досягти максимально можливої довіри при використанні звичайних методів розробки. Його застосовують тоді, коли розробникам або споживачам потрібен середній рівень довіри на основі всебічного дослідження системи та процесу її розробки.

Порівняно з Другим рівнем тут додається вимога, яка змушує розробника розробити акт про випробування з урахуванням особливостей не тільки функціональної специфікації, але й проекту вищого рівня. Крім того, вимагається контроль середовища розробки та керування конфігурацією системи.

Четвертий рівень довіри передбачає систематичне проектування, тестування та спостереження. Вони допомагають досягти максимально можливої довіри за умови стандартної практики комерційних розробок. Це максимально можливий рівень довіри, на який, напевне, економічно доцільно орієнтуватися для існуючих типів продуктів.

Четвертий рівень характеризується аналізом функціональної специфікації, повної специфікації інтерфейсів, експлуатаційної документації, проектів вищого та нижнього рівнів, а також підмножини реалізації; необхідно також застосовувати неформальну політику безпеки системи. Додаткові вимоги – незалежний аналіз вразливостей, який демонструє стійкість системи до спроб проникнення порушників з низьким потенціалом, та автоматизація керування конфігурацією.

П’ятий рівень довіри вимагає напівформального проектування та тестування. З його допомогою досягається максимально можлива довіра для строгої практики комерційної розробки, яка підтримується помірним застосуванням спеціалізованих методів забезпечення захисту. Цей рівень використовують, коли потрібен високий рівень довіри та строгий підхід до розробки, який не несе зайвих витрат. Для досягнення п’ятого рівня вимагається формальна політика безпеки системи та напівформальне представлення функціональної специфікації та проекту вищого рівня, напівформальна демонстрація відповідності між ними, а також модульна структура проекту системи. Необхідна стійкість до спроб проникнення порушників з середнім потенціалом; передбачається також перевірка правильності аналізу прихованих каналів розробником та всебічне керування конфігурацією.

Шостий рівень довіри характеризується напівформальною верифікацією проекту. Він дозволяє отримати високу довіру застосування спеціальних методів проектування у строго контрольованому середовищі розробки, яке застосовується для виробництва високоякісних виробів інформаційних технологій та для захисту цінних активів від значних ризиків. Шостий рівень довіри має такі особливості: структуроване представлення реалізації; напівформальне представлення проекту нижнього рівня; ієрархічна структура проекту системи; стійкість до спроб проникнення порушників з високим потенціалом;перевірка правильності систематичного аналізу прихованих каналів розробником; використання структурованого процесу розробки;повна автоматизація керування конфігурацією.

Сьомий рівень довіри вимагає формальну верифікацію проекту. Він застосовується до розробки виробів інформаційних технологій для використання в ситуаціях надзвичайно високого ризику або там, де висока цінність активів виправдовує підвищені витрати.

На додаток до шостого рівня, на сьомому вимагають:

– формальне представлення функціональної специфікації та проекту верхнього рівня, формальна демонстрація відповідності між ними;
– модульна, ієрархічна та проста структура проекту системи;
– додавання представлення реалізації як основи акту випробувань;
– повне незалежне підтвердження результатів тестування розробником.

Рівні довіри ЗК, на думку аналітиків обрані досить вдало. Тому вважається, що їх підсилення, в разі необхідності, може носити непринциповий характер.

5.3 НД ТЗІ 2.5-004-99

Цей нормативний документ встановлює критерії оцінки захищеності інформації, яка обробляється комп’ютерними системами, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог із захисту інформації; створення захищених комп’ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп’ютерних системах та їх придатності для обробки інформації, що потребує захисту. Критерії надають: метрику для оцінки надійності механізмів захисту інформації від несанкціонованого доступу; базу для розробки комп’ютерних систем, де повинні бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до усього спектру комп’ютерних систем і призначаються для розробників, споживачів комп’ютерних систем, які використовуються для обробки критичної інформації, а також для органів, що

виконують оцінювання захищеності такої інформації та контроль за її обробкою.

Структуру критеріїв подана на рисунку 5.1. З цього рисунку видно, що у нормативному документі розглядаються вимоги двох типів: вимоги до функцій захисту (або послуг безпеки); вимоги до гарантій.

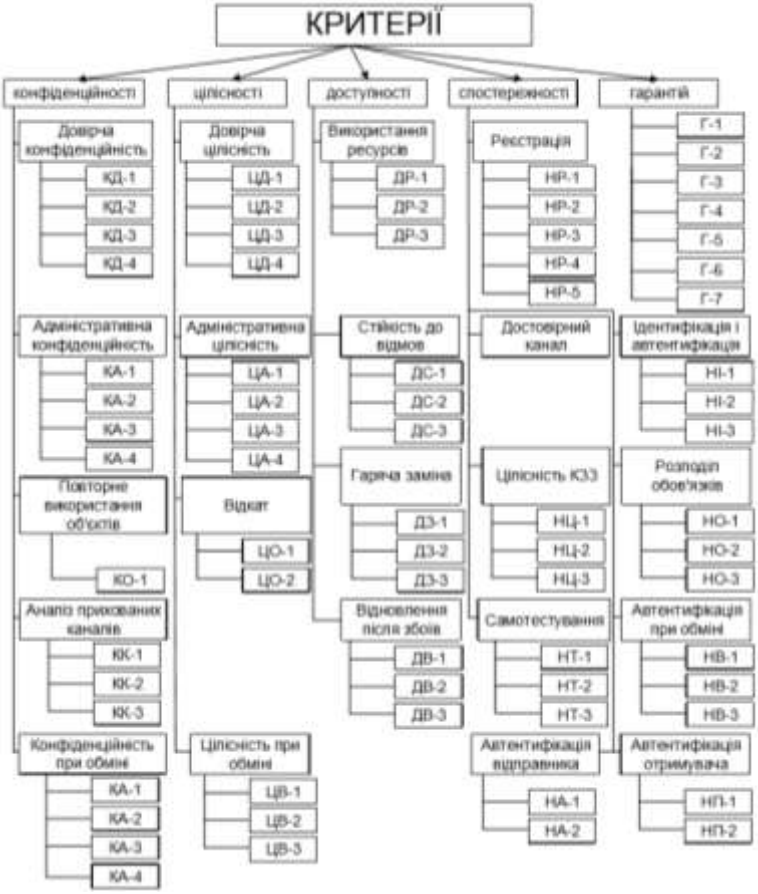

Рисунок 5.1 – Структура критеріїв НД ТЗІ 2.5-004-99

Комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга є набором функцій, що дозволяють протистояти певній сукупності загроз і включає кілька рівнів. Чим вищий рівень послуги, тим повніше забезпечується захист від певного типу загроз.

Функціональні критерії розбито на чотири групи, кожна з яких визначає вимоги до захисту від загроз одного з чотирьох основних типів.

Конфіденційність. Загрози, пов'язані з несанкціонованим ознайомленням з інформацією, становлять загрози конфіденційності. У цьому розділі описано такі послуги, як довірча конфіденційність; адміністративна конфіденційність; повторне використання об'єктів; аналіз прихованих каналів; конфіденційність при обміні (експорті та імпорті).

Цілісність. Загрози несанкціонованої модифікації інформації становлять загрози цілісності. В цьому розділі описано такі послуги: довірча цілісність; адміністративна цілісність; відкат і цілісність при обміні.

Доступність. Загрози, що стосуються порушення можливості використання комп'ютерних систем або інформації, що обробляється ними, становлять загрози доступності. В цьому розділі описано такі послуги, як використання ресурсів, стійкість до відмов, гаряча заміна та відновлення після збоїв.

Спостережність. Ідентифікація та контроль за діями користувачів, керування комп'ютерною системою становлять предмет послуг спостережності та керованості. У цьому розділі описано такі послуги: реєстрація, ідентифікація та автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, саме тестування, автентифікація при обміні, автентифікація відправника (неможливість відмови від авторства), автентифікація одержувача (неможливість відмови від одержання).

Окрім функціональних критеріїв цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту (КЗЗ); середовища розробки; випробування КЗЗ; середовища функціонування та експлуатаційної документації. У Критеріях уведено сім ієрархічних рівнів гарантій, що нагадує Загальні критерії. Ієрархія рівнів гарантій надає споживачеві міру впевненості в тому, що система безпеки здатна протистояти актуальним загрозам інформації. Ця впевненість зростає зі збільшенням номеру рівня гарантій.

Усі послуги до деякої міри незалежні. Якщо ж така залежність виникає, тобто реалізація деякої послуги неможлива без реалізації іншої, цей факт відображено як необхідну умову для даної послуги або рівня. За винятком послуги аналіз прихованих каналів залежність між функціональними послугами і гарантіями відсутня. Однак рівень послуги «Цілісність КЗЗ» НЦ-1 – необхідна умова абсолютно для всіх рівнів усіх інших послуг. Порядок оцінки комп'ютерної системи щодо відповідності цим Критеріям визначається відповідними нормативними критеріями, зокрема, НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі». Експертна

комісія повинна визначити, які послуги і на якому рівні реалізовано в комп'ютерній системі, що оцінюється, і як дотримуються вимог гарантій. Результатом оцінки є рейтинг, тобто перелік комбінацій, які позначають рівні реалізованих послуг разом з рівнем гарантій. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, необхідно виконати усі вимоги цього рівня.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. У чому полягає суть системи безпеки за «Оранжевою книгою»?
2. Які критерії захищеності комп'ютерних систем передбачено європейським стандартом?
3. Вимоги довіри, які висуваються до етапів життєвого циклу системи безпеки.
4. У чому полягає суть національного стандарту у галузі оцінки захищеності комп'ютерних систем?
5. Послуги та механізми безпеки інформаційних систем.
6. Які вимоги, у відповідності до європейського стандарту, висуваються до постачання, експлуатації та підтримки довіри?
7. Функціональні вимоги безпеки.
8. Рівні оцінки довіри.
9. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу.
10. Функціональні критерії та їх вимоги до захисту від загроз.

Література: [2; 5-11; 14-17].

Тема 6. Шифрування даних

План:

6.1 Теорія зв'язку в секретних системах

6.2 Симетричні, асиметричні та комбіновані криптосистеми

6.3 Основні вимоги, які висуваються до сучасних криптосистем

На сьогодні, завдання захисту інформації в комп'ютерних системах є однією із найактуальніших задач, внаслідок широкого розповсюдження таких систем, а також розширення локальних і глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення сторонніх осіб з цією інформацією.

Не менш важливим завданням є широке впровадження у різні сфери діяльності людини електронного документообігу, який повинен забезпечуватися юридичною чинністю підписаних електронних документів.

Усі ці та багато інших завдань захисту інформації покликана вирішувати криптографія.

Криптографічні механізми настільки тісно пов'язані із сучасними інформаційними технологіями, що разом з підвищенням комп'ютерної грамотності необхідно опановувати основи криптографії.

Грецьке слово «cryptos» перекладається як «таємниця», а отже, криптографія означає тайнопис. Звідси випливає, що початковим завданням криптографії було розроблення методів, які спрямовано на приховування змісту переданої або збереженої інформації. І хоча на цей час сфера застосування криптографічних механізмів значно розширилася, основні ідеї полягають у забезпеченні конфіденційності інформації.

Варто зазначити, що кожному етапові розвитку цивілізації властиві відповідні криптографічні пристрої. Тривалий час шифрування текстів виконувалося вручну. Їх створення можна було вважати скоріше мистецтвом, ніж якоюсь стандартною процедурою. Відомо два протилежні погляди щодо шифрів. Відповідно до першого можна створити шифр, який неможливо розкрити. Другий полягає у тому, що малоймовірно, що «загадку», яка лежить в основі створеного шифру, не можна розгадати.

Згодом науку про перетворення інформації у незрозумілу для сторонніх осіб форму стали називати криптографією. Методи пошуку «розгадки» стали називати крипто-аналітичними методами, а відповідну галузь досліджень – крипто-аналізом. Отже, криптоаналіз – це наука, спрямована на подолання криптографічного захисту.

Тепер усе ширше використовують термін криптологія, тобто наука про шифри. Вважають, що криптологію складають дві великі частини, які доповнюють одна одну, – криптографія та криптоаналіз.

Процес криптографічного перетворення інформації прийнято називати шифруванням (або зашифруванням, як це часто використовується у криптологічній літературі). Зашифровану інформацію повинні прочитати ті особи, для кого призначена ця інформація. Перш ніж прочитати, її треба перетворити у зрозумілу форму. Цей процес, який називається розшифруванням, виконується за допомогою деякої секретної частини криптографічної системи – криптографічного ключа (або просто ключа).

Зловмисник, який перехопив зашифровану інформацію, як правило, не має

такого ключа. Тому він намагається подолати криптографічний захист за допомогою криптоаналітичних методів. Такий спосіб, тобто розшифрування повідомлення без знання ключа, називають дешифруванням. Отже, можна сказати, що розшифровують «свої», а дешифрують – «чужі».

Методи криптографічного захисту інформації можуть реалізовуватися як апаратно, так і програмно. Апаратна реалізація має суттєво більшу вартість, однак водночас і більшу продуктивність та захищеність. Програмна реалізація практичніша, дешевша та гнучкіша у використанні.

6.1 Теорія зв'язку в секретних системах

Клод Елвуд Шеннон, у роботі «Теорія зв'язку в секретних системах» зробив визначальний внесок у сучасну криптографічну науку. Прийнято вважати, що ця робота, яка була спершу його секретною доповіддю «Математична теорія криптографії» (1945 р.), була розсекречена після Другої світової війни (1949 р.), визначила основи та сформувала обличчя сучасної криптографії.

К. Шеннон народився у 1916 р. в м. Гейлорді (США). У 1936 році він закінчив Масачусетський технологічний інститут, спеціалізуючись одночасно на математиці та електротехніці. У 1941 р. К. Шеннона запросили на роботу в Bell Laboratories, де у роки війни він займався розробкою криптографічних систем, що пізніше допомогло йому відкрити методи кодування з корекцією помилок.

Метою К. Шеннона була оптимізація передавання інформації телефонними та телеграфними лініями. Для того, щоб вирішити цю проблему, йому довелося сформулювати, що ж таке інформація, чим визначається її кількість. У своїх роботах 1948-49 років він визначив кількість інформації через ентропію – величину, яка використовується у термодинаміці та статистичній фізиці як міра розупорядкованості системи, а за одиницю інформації – величину, яку потім було названо «бітом», тобто вибір з двох рівноймовірних варіантів. К. Шеннон розглядає шифрування, як відображення відкритого тексту в шифрограму:

$$C=F_i(M),$$

де C – шифрограма;

M – відкритий текст;

F_i – відповідне відображення, індекс «і» відповідає конкретному криптографічному ключу, використаному при шифруванні.

Для того, щоб існувала можливість однозначного розшифрування повідомлення, відображення F_i повинно мати єдине обернене відображення F_i^{-1}, таке, що $F_iF_i^{-1}=I$ (де I – тотожне перетворення):

$$M=F_i^{-1}(C).$$

Враховано, що джерело ключів є статистичним процесом або пристроєм, який задає відображення F_1, F_2, …, F_N із імовірностями $p_1,p_2,\ldots,p_N$.

Розглянемо найпростіший шифр, де вихідна абетка повідомлень співпадає із множинами знаків ключа та криптограми, а шифрування виконується послідовною заміною знаків відкритого тексту знаками криптограми залежно від чергового значення знаків ключа.

У цьому випадку відкритий текст, ключ і криптограма є послідовностями літер того самого алфавіту: $M=(m_1m_2m_3\ldots m_n)$; $K=(k_1k_2k_3\ldots kn)$; $C=(c_1c_2c_3\ldots c_n)$. Кожен крок шифрування визначається співвідношенням $c_i=f(m_i, k_i)$.

У практичних криптосистемах довжина ключа значно менша за довжину відкритого тексту, тому часто ключова послідовність може обчислюватися за допомогою деякого первісного ключа меншого розміру або навіть може бути періодичною.

Завдання криптоаналітика полягає в обчисленні відкритого тексту за криптограмою, знаючи множину відображень F_1, F_2, …, F_N.

Існують криптосистеми, для яких будь-який об'єм перехопленої інформації недостатній для знаходження шифрувального відображення, причому ситуація не залежить від обчислювальної потужності обладнання криптоаналітика. Шифри такого типу називаються безумовно стійкими (ідеально секретними). Строго кажучи, безумовно стійкими будуть такі шифри, для яких криптоаналітик, навіть маючи безмежні обчислювальні ресурси, не зможе покращити оцінку вихідного повідомлення (відкритого тексту) M, знаючи криптограму C, порівняно із оцінкою при невідомій криптограмі. Це можливо лише тоді, коли M і C є статистично незалежними. Безумовно, стійкі криптосистеми існують.

Нехай у розглянутому простому шифрі використовується абетка із L літер, а поточні знаки криптограми генеруються за законом:

$$c_i=f(m_i, k_i)=(m_i+k_i)\text{mod}L,$$

де для кожного знаку c_i, m_i, k_i поставлено у відповідність їх порядковий номер в абетці.

Оберемо в якості ключа послідовність з n випадкових знаків $k_1k_2k_3\ldots k_n$, тобто виберемо випадковий ключ, розмір якого дорівнює довжині повідомлення. Для генерування ключа використаємо деякий фізичний генератор випадкових чисел, що забезпечує рівну імовірність кожного елемента з множини чисел {1, 2, …, N}. Обране джерело забезпечує рівноймовірність вибору будь-якого ключа довжини n. У цьому випадку імовірність вибору ключа довжини n

складає:

$$P(K=K_i)=L^{-n}.$$

З цього виразу видно, що для довільних M і C виконується аналогічне співвідношення:

$$P(M=M_i/C=C_i)=L^{-n}.$$

А це, у свою чергу, означає, що криптограмі довжини n з імовірністю L^{-n} може відповідати будь-який відкритий текст довжини n.

Для шифрування іншого повідомлення оберемо інший випадковий ключ. Така процедура шифрування забезпечує безумовну стійкість. Криптосистеми, що використовують рівно ймовірний випадковий ключ, що має рівну з відкритим текстом довжину, називаються шифрами зі стрічкою одноразового використання або шифрами з безмежною ключовою гамою. На практиці такі системи отримали лише обмежене використання, оскільки досить незручні у використанні.

Криптосистеми іншого типу характеризуються тим, що при зростанні кількості доступної для крипто-аналітика інформації, при певному значенні $n=n_0$ існує єдиний розв'язок крипто-аналітичної задачі. Мінімальний об'єм криптограми, для якого існує єдиний розв'язок, називається інтервалом єдності. У випадку стрічки одноразового використання $n_0 \to \infty$. За кінцевої довжини криптографічного ключа значення n_0 кінцеве.

Відомо, що за криптограмою, довжиною, більшою за інтервал єдності, можна знайти цей єдиний розв'язок. Однак для крипто-аналітика з обмеженими обчислювальними ресурсами, імовірність знайти цей розв'язок за скінчений проміжок часу (поки інформація має ще якусь цінність) надзвичайно мала (10-30 й менше). Шифри такого типу називаються умовно стійкими (практично стійкими). Їх стійкість ґрунтується на значній обчислювальній складності розв'язку крипто-аналітичної задачі.

Мета розробника умовно стійких криптосистем полягає в тому, щоб зменшити витрати на процедури шифрування та розшифрування, і одночасно задати такий рівень складності крипто-аналітичної задачі, щоб для успішного розв'язку її потрібно було залучити такі ресурси, вартість яких перетворювала знаходження рішення в економічно невигідну задачу.

Завдання такого об'єму обчислень називаються важкими або обчислювально складними, а про їх розв'язок говорять, що вони обчислювально нездійсненними. Шифри, які ґрунтуються на обчислювально нездійсненних задачах, називаються обчислювально стійкими. Найбільшу практичну розповсюдженість мають якраз обчислювально стійкі криптосистеми.

Під стійкістю криптосистем такого роду будемо розуміти складність розв'язку криптоаналітичної задачі при певних умовах. К. Шеннон увів поняття робочої характеристики W(n) шифру як середню кількість роботи для знаходження ключа за відомими n знаками криптограми з використанням найкращого алгоритму криптоаналізу. Кількість роботи можна виміряти, наприклад, кількістю операцій, які необхідно виконати для обчислення ключа. Цей параметр безпосередньо пов'язаний із алгоритмом обчислення ключа. Складність визначення W(n) пов'язана зі складністю знаходження найкращого способу розкриття. Особливо цікавим є граничне значення W(n) для $n \to \infty$.

На даний час про обчислювально стійкі криптосистеми, для яких обчислено $W(\infty)$, нічого не відомо. Внаслідок складності такої оцінки, практичні шифри характеризують досягнутою оцінкою робочої характеристики, яку отримують для найкращого з відомих сьогодні методів обчислення ключа.

К. Шеннон запропонував також модель для оцінки інтервалу єдиності, із якої отримано співвідношення:

$$n_0 = H(K)/D,$$

де H(K) – ентропія ключа, яка для випадкового ключа дорівнює довжині ключа в бітах;

D – надмірність мови, яка вимірюється у бітах на знак.

Це співвідношення можна записати у наступному вигляді:

$$H(K) \le n^D,$$

де H(K) характеризує кількість невідомих у двійковому представленні ключа;

nD – кількість рівнянь для обчислення ключа.

Якщо кількість рівнянь менше за кількість невідомих, розв'язок системи буде неоднозначним. У таких умовах криптосистема буде безумовно стійкою. Якщо кількість рівнянь більша кількості невідомих, то існує єдиний розв'язок, а криптосистема не вважається безумовно стійкою. Однак вона може бути обчислювально стійкою, якщо $n >> n0$. Рівень стійкості обчислювально стійких криптосистем залежить від типу шифрувальних процедур. Конкретні процедури перетворення також визначає хід робочої характеристики, тобто явний вигляд залежності W(n).

6.2 Симетричні, асиметричні та комбіновані криптосистеми

Симетричні криптосистеми. На рисунку 6.1 подано загальну схему

симетричної, або традиційної, криптографії.

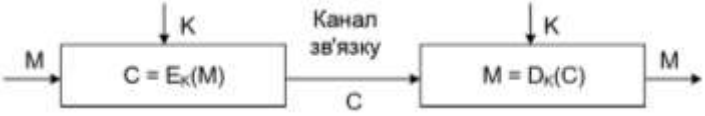

Рисунок 8.1 – Загальна схема симетричного шифрування

У процесі шифрування використовується певний алгоритм шифрування, на вхід якому подаються незашифроване повідомлення (англ. – plaintext) і ключ шифрування. Виходом алгоритму є зашифроване повідомлення шифротекст (англ. – ciphertext). Ключ шифрування є значенням, що не залежить від незашифрованого повідомлення. Зміна ключа повинна призводити до зміни зашифрованого повідомлення.

Зашифроване повідомлення передається одержувачу. Одержувач перетворює зашифроване повідомлення у вихідне незашифроване за допомогою алгоритму розшифрування і того ж самого ключа, який використовувався при шифруванні, або ключа, який можна легко одержати з ключа шифрування.

Незашифроване повідомлення варто позначати P або M, від слів plaintext та message (англ. – повідомлення). Зашифроване повідомлення прийнято позначати через C, від слова ciphertext.

Стійкість, яку забезпечує традиційна криптографія, залежить від декількох чинників.

По-перше, криптографічний алгоритм повинен бути досить сильним, щоб передане зашифроване повідомлення неможливо було розшифрувати без ключа, використовуючи тільки різні статистичні закономірності зашифрованого повідомлення або які-небудь інші способи його аналізу.

По-друге, безпека переданого повідомлення повинна залежати від секретності ключа, але не від секретності алгоритму. Алгоритм повинен бути проаналізований фахівцями, і позбавлений слабких місць, через які можна відновити погано прихований зв'язок між відкритим і зашифрованим повідомленнями. До того ж для стійких алгоритмів виробники можуть створювати дешеві апаратні засоби або вільно розповсюджувані програми, що реалізують цей алгоритм шифрування.

По-третє, алгоритм повинен бути настільки довершеним, щоб не можна було обчислити ключ, навіть знаючи досить багато пар зашифроване повідомлення-незашифроване повідомлення, отриманих при шифруванні з використанням цього ключа.

К. Шеннон ввів поняття дифузії і конфузії для опису стійкості алгоритму шифрування.

Дифузія – це розсіювання статистичних особливостей відкритого тексту в широкому діапазоні статистичних особливостей зашифрованого тексту. Дифузія досягається тим, що значення кожного елемента відкритого тексту впливає на значення багатьох елементів зашифрованого тексту або, що те ж саме, будь-який елемент зашифрованого тексту залежить від багатьох елементів відкритого тексту.

Конфузія – це знищення статистичного взаємозв'язку між зашифрованим текстом і ключем.

Стандартний алгоритм шифрування повинен бути таким, щоб його можна було успішно використовувати в багатьох галузях: для шифрування даних або потоків даних; для створення певної кількості випадкових бітів; легко перетворюватися в однобічну геш-функцію. Стандартний алгоритм шифрування повинен дозволяти реалізацію на різних платформах, які висувають різні вимоги, в тому числі на спеціалізованій апаратурі шифрування/дешифрування. Додатковими вимогами до стандартних алгоритмів можуть бути: алгоритм повинен бути простим для програмної реалізації, щоб мінімізувати імовірність програмних помилок; простір ключів має бути плоским; алгоритм повинен мати можливість використання довільного випадкового рядка бітів у якості можливого ключа; наявність слабких ключів небажана; алгоритм повинен легко модифіковуватися для різних рівнів безпеки; бажано, щоб усі операції з даними виконувалися над блоками, кратними або байту, або 32-бітному слову.

Алгоритми симетричного шифрування відрізняються способом, яким обробляється вихідний текст. Можливе шифрування блоками або шифрування потоком. Блок тексту розглядається як додатне ціле число, або як кілька незалежних додатних цілих чисел. Довжина блоку завжди дорівнює 2n. У більшості блокових алгоритмів симетричного шифрування використовуються такі типи операцій:

– таблична підстановка, коли група бітів відображується в іншу групу бітів (так звані S-box);

– перестановки, за допомогою яких біти повідомлення перемішуються (так звані P-box);

– операція додавання за модулем 2 (XOR або $\oplus$);

– операція додавання за модулем 232 або за модулем 216;

– циклічний зсув на певну кількість бітів.

Ці операції циклічно повторюються в алгоритмі, утворюючи так звані

раунди. Входом кожного раунду є вихід попереднього раунду і ключ, отриманий за певним алгоритмом з ключа шифрування K.

Критерії, використані при розробці алгоритмів. Беручи до уваги перераховані вимоги, вважають, що алгоритм симетричного шифрування повинен:

– маніпулювати даними в більших блоках, переважно розміром 16 або 32 біти;

– мати розмір блоку 64÷256 бітів;

– мати масштабований ключ до 256 бітів;

– використовувати прості операції, ефективні на мікропроцесорах, що виключають додавання, табличні підстановки, або множення за модулем;

– не повинні використовуватися зсув змінної довжини, побітні перестановки або умовні переходи;

– повинна бути можливість реалізації алгоритму на 8-бітному процесорі із мінімальними вимогами до пам'яті;

– використовувати заздалегідь обчислені підключі (при неможливості попереднього обчислення підключів можливе лише зменшення швидкодії або завжди повинна бути можливість шифрування даних без яких-небудь попередніх обчислень).

Складатися зі змінного числа ітерацій. Для застосувань з маленькою довжиною ключа недоцільно використовувати велику кількість ітерацій для протистояння диференціальним й іншим атакам. Отже, повинна бути можливість зменшити число ітерацій без значної втрати стійкості.

По можливості не мати слабких ключів. Якщо це неможливо, то кількість слабких ключів повинна бути мінімальною, щоб зменшити ймовірність випадкового вибору одного з них. Проте усі слабкі ключі повинні бути заздалегідь відомі, щоб їх можна було відбракувати в процесі створення ключа.

Задіяти підключі, які є однобічним гешем ключа. Це дає можливість використовувати довші парольні фрази без шкоди для безпеки.

Не мати лінійних структур, які зменшують лінійну складність. Алгоритм повинен бути простим для розуміння, що спрощує його аналіз та пошук слабких місць. Більшість блокових алгоритмів ґрунтується на використанні сітки Фейстеля, всі мають плоский простір ключів і дозволяють відбраковку слабких ключів.

Ключ раунду називається підключем. Кожний симетричний алгоритм шифрування може бути схожим на той, який подано на рисунку 6.2.

Асиметричні криптосистеми. Якими б не були надійними симетричні

криптоалгоритми, слабким місцем їх практичної реалізації залишається проблема розподілу криптографічних ключів. Для безпечного обміну інформацією між двома суб'єктами, один з них повинен згенерувати ключ та якимось чином конфіденційно передати іншому. Таким чином, для передавання криптографічного ключа необхідно використати або існуючу криптосистему, або захищений інформаційний канал. Однак тут постає питання: якщо суб'єкти мають захищений інформаційний канал, то чи не можна використати його для передавання самої інформації? Зрозуміло, що це досить незручно та дорого.

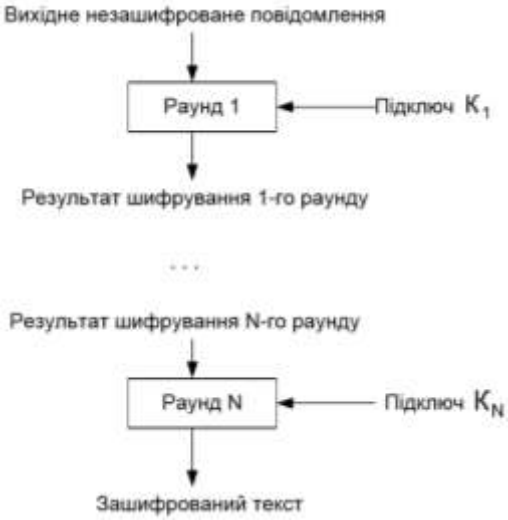

Рисунок 8.2 – Структура симетричного алгоритму

Для вирішення цієї проблеми на основі нових результатів сучасної алгебри було запропоновано системи з публічним ключем (асиметричні криптосистеми).

Суть таких систем, як уже зазначалося, полягає в тому, що кожним суб'єктом інформаційного обміну генеруються два ключа, зв'язані між собою певними правилами. Один ключ оголошується публічним (відкритим), а інший – приватним (секретним). Публічний ключ розміщується на доступному усім ресурсі (публікується), тому він доступний для усіх учасників інформаційного обміну. Приватний ключ зберігається суб'єктом, який його створив, і недоступний для інших суб'єктів.

Відкритий текст зашифровується на публічному ключі та передається адресатові. Зашифрований текст не може бути розшифрований на публічному ключі (в усякому разі для досить довгих ключів це обчислювально дуже складна

процедура). Розшифрування повідомлення можливо лише на відповідному приватному ключі, відомому лише безпосередньо адресату.

Асиметричні криптосистеми, як вже зазначалося, використовують так звані односторонні функції, які мають таку властивість: при заданому значенні x відносно легко обчислити значення f(x), однак якщо відомо значення y=f(x), то не існує простого способу обчислення значення x. Велика кількість класів незворотних функцій і породжують усю різноманітність криптосистем з відкритим ключем. Однак в самому означенні є деяка невизначеність: яка означає «не існує простого способу».

Тому для асиметричних криптосистем ставляться дві важливих вимоги: перетворення відкритого тексту повинно бути незворотним без можливості його відновлення на публічному ключі; обчислення приватного ключа на основі публічного також повинно бути неможливим на сучасному технологічному рівні.

При цьому бажаною є точна нижня оцінка трудомісткості розкриття шифру. Алгоритми шифрування з відкритим ключем використовують у трьох напрямах:

– як самостійні засоби захисту інформації;
– як засоби автентифікації користувачів;
– як засоби розповсюдження ключів.

Справа у тому, що внаслідок особливостей математичних розрахунків, асиметричні криптоалгоритми значно повільніші за симетричні. Тому часто на практиці раціонально використати перші для шифрування невеликої кількості інформації, а потім за допомогою симетричних алгоритмів виконувати шифрування великих інформаційних потоків.

Комбінований метод шифрування. Головною перевагою криптосистем з відкритим ключем є їх потенційно висока безпека: немає необхідності ні передавати, ні повідомляти будь-кому значення секретних ключів, ні переконуватись в їх дійсності.

У симетричних криптосистемах існує небезпека розкриття секретного ключа під час передачі.

Однак алгоритми, що лежать в основі криптосистем з відкритим ключем, мають такі недоліки:

– генерація нових секретних і відкритих ключів заснована на генерації нових великих простих чисел, а перевірка простоти чисел займає багато процесорного часу;

– процедури шифрування і розшифрування, пов’язані зі зведенням у степінь багатозначного числа, досить громіздкі.

Тому швидкодія криптосистем із відкритим ключем на 2-5 порядків разів менша за швидкодію симетричних криптосистем з секретним ключем.

Комбінований (гібридний) метод шифрування дозволяє поєднувати переваги високої таємності, надавані асиметричними криптосистемами з відкритим ключем, з перевагами високої швидкості роботи, властивими симетричним криптосистемам із секретним ключем. При такому підході криптосистема з відкритим ключем застосовується для шифрування, передачі і наступного розшифрування тільки секретного ключа симетричної криптосистеми. А симетрична криптосистема застосовується для шифрування і передачі вихідного відкритого тексту. У результаті криптосистема з відкритим ключем не заміняє симетричну криптосистему із секретним ключем, а лише доповнює її, дозволяючи підвищити в цілому захищеність інформації, яка передається. Такий підхід іноді називають схемою електронного цифрового конверту.

Якщо користувач А прагне передати зашифроване комбінованим методом повідомлення М користувачу В, то порядок його дій буде таким, як наведено нижче.

1. Створити (наприклад, згенерувати випадковим чином) симетричний ключ, названий у цьому методі сеансовим ключем K_s.

2. Зашифрувати повідомлення М на сеансовому ключі K_s.

3. Зашифрувати сеансовий ключ K_s на відкритому ключі K_B користувача В.

4. Передати відкритим каналом зв'язку на адресу користувача В зашифроване повідомлення разом із зашифрованим сеансовим ключем.

Дії користувача В при одержанні зашифрованого повідомлення і зашифрованого сеансового ключа повинні бути зворотними:

5. Розшифрувати на своєму секретному ключі K_B сеансовий ключ K_s.

6. За допомогою отриманого сеансового ключа K_s розшифрувати і прочитати повідомлення М.

При використанні комбінованого методу шифрування можна бути впевненим у тому, що тільки користувач В зможе правильно розшифрувати ключ K_s і прочитати повідомлення М. Таким чином, при комбінованому методі шифрування застосовуються криптографічні ключі як симетричних, так і асиметричних криптосистем. Очевидно, що вибір довжин ключів для кожного типу криптосистеми слід здійснювати таким чином, щоб зловмиснику було однаково важко атакувати будь-який механізм захисту комбінованої криптосистеми. У таблиці 6.1 наведено найбільш розповсюджені довжини ключів симетричних і асиметричних криптосистем, для яких труднощі атаки

повного перебору приблизно дорівнюють труднощам факторизації відповідних модулів асиметричних криптосистем.

Таблиця 6.1 – Довжини ключів для симетричних і асиметричних криптосистем

Довжина ключа симетричної криптосистеми, біти	Довжина ключа асиметричної криптосистеми, біти
56	384
64	512
80	768
112	1792
128	2304

Комбінований метод допускає можливість виконання процедури автентифікації, тобто перевірки дійсності переданого повідомлення. Для цього користувач А на основі функції гешування повідомлення і свого секретного ключа kA за допомогою відомого алгоритму електронному цифровому підпису генерує свій підпис і записує її, наприклад, у кінець переданого файла.

Користувач В, прочитавши прийняте повідомлення, може переконатися в дійсності цифрового підпису абонента А. Використовуючи той же алгоритм ЕЦП і результат гешування прийнятого повідомлення, користувач В перевіряє отриманий підпис. Комбінований метод шифрування є найбільш раціональним, поєднуючи в собі високу швидкодію симетричного шифрування та високу криптостійкість, яка гарантується системами з відкритим ключем.

6.3 Основні вимоги, які висуваються до сучасних криптосистем

Абстрактно секретна система визначається, як деяка множина відображень одного простору (множини можливих повідомлень) в інший простір (множину можливих криптограм).

Зафіксуємо множину можливих повідомлень $M=\{M_1, M_2, \ldots, M_m\}$ і множину криптограм $E=\{E_1, E_2, \ldots, E_n\}$. Зафіксуємо також множину відображень $\varphi=\{\varphi_1, \varphi_2, \ldots, \varphi_k\}$, де $\varphi_i: M \rightarrow E$: i=1, 2, …, k.

Якщо множини М та Е рівнопотужні, тобто n=m, а відображення $\varphi_i \in \varphi$ сюр'єктивне та ін'єктивне, то існує обернене відображення $\varphi_i^{-1}: E \rightarrow M$, що кожному елементу множини Е ставить у відповідність елемент множини М.

Очевидно, що φі та φ_i^{-1} задають взаємно однозначне відображення множин М та Е.

Зафіксуємо тепер множину ключів $K=\{K_1, K_2, \ldots, K_k\}$ так, що для всіх i=1, 2, …, k відображення $\varphi_i \in \varphi$ однозначно задається ключем K_i, тобто:

$$\varphi_i : M \xrightarrow{K_i} E.$$

Кожне відображення φ_i з множини відповідає способу шифрування за допомогою конкретного ключа K_i. На рисунку 6.3 схематично подано відображення $\varphi_i \in \varphi$ φ задане ключем K_i.

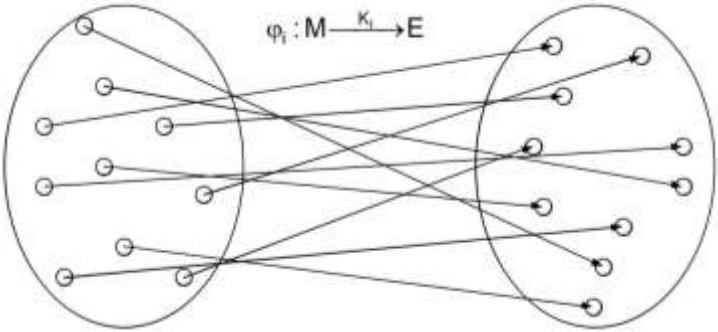

Рисунок 6.3 – Відображення φ_i^{-1} множини відкритих текстів у множину криптограм

Зафіксуємо множину ключів $K^*=\{K_1^*, K_2^*, \ldots, K_k^*\}$ у загальному $K_i^* \in K^*$. Усі елементи множини зворотних відображень φ-1$=\{\varphi_1^*, \varphi_2^*, \ldots, \varphi_k^*\}$ задаються відповідним ключем $\varphi_i^{-1} : M \xrightarrow{K_i} E.$

Кожне конкретне відображення φ_i^{-1} з множини φ^{-1} відповідає способу розшифрування за допомогою ключа K_i^*.

Якщо відомо ключ K_i^*, то в результаті розшифрування можлива єдина відповідь – елемент множини M.

Таким чином, в абстрактне визначення криптосистеми входять такі множини: M, E, φ_i, φ^{-1}, K, K^* (множини відкритих текстів і криптограм, множини прямих і обернених відображень, множини ключів).

Якщо при цьому $K \neq K^*$, то система асиметрична, і навпаки, якщо $K=K^*$ – симетрична. Відповідно до принципу Кірхгофа стійкість секретної системи повинна базуватися тільки на збереженні в таємниці від противника ключа, а не на секретності алгоритму шифрування.

На рисунку 6.4 подано структурну схему секретної системи. Джерело повідомлень породжує потік повідомлень із множини M. Кожне повідомлення зображується конкретною реалізацією деякого випадкового процесу, що описує роботу джерела повідомлень. Кожному повідомленню $M_i \in M=\{M_1, M_2, \ldots, M_m\}$

відповідає ймовірність $P(M_i)$. Розподіл ймовірностей випадкового процесу задається сукупним розподілом ймовірностей випадкових величин:

$$P_M=\{P(M_1), P(M_2), \ldots, P(M_m)\}.$$

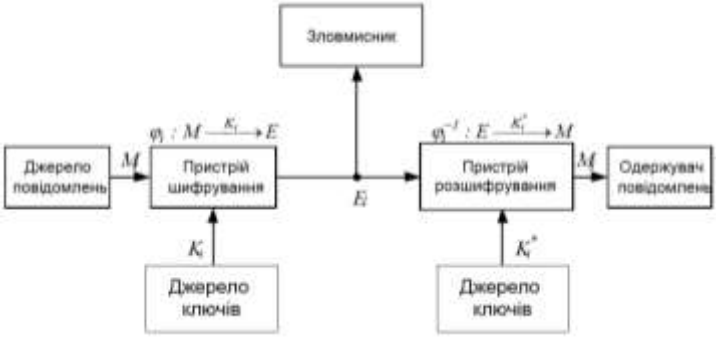

Рисунок 6.4 – Структурна схема секретної системи

Джерело ключів породжує потік ключів з множини K і/або K^*. Кожному ключу $K_i \in K=\{K_1, K_2, \ldots, K_k\}$ відповідає деяка ймовірність $P(K_i)$, а кожному $K_i^* \in K^*=\{K_1^*, K_2^*, \ldots, K_k^*\}$ – ймовірність $P(K_i^*)$. Випадковий процес генерування ключів задається множинами:

$$P_K=\{P(K_1), P(K_2), \ldots, P(K_k)\};$$

$$P_K^*=\{P(K_1^*), P(K_2^*), \ldots, P(K_k^*)\}.$$

Ці множини утворюють апріорні знання зловмисника про джерело повідомлень і ключів відповідно. Фактично ці множини характеризують апріорні знання супротивника щодо можливої «слабкості» секретної системи.

Вибір ключа K_i визначає конкретне відображення φ_i з множини відображень φ. Криптограма тоді буде формуватися таким чином:

$$E_I=\varphi_i(K_i, M_i).$$

Криптограма E_I передається на приймальну сторону деяким каналом й може бути перехоплена супротивником. На приймальному кінці за допомогою оберненого відображення φ_i^{-1} (заданого ключем K_i^*) із криптограми E_I відновлюється відкрите повідомлення:

$$M_I=\varphi_i^{-1}(K_i^*, E_i).$$

Якщо супротивник перехопить криптограму EI, він може з її допомогою спробувати обчислити апостеріорні ймовірності різних можливих повідомлень:

$$P_{M|EI}=\{P(M_1|E_I), P(M_2|E_I), \ldots, P(M_m|E_I)\},$$

і різних можливих ключів:

$$P_{K|EI}=\{P(K_1|E_I), P(K_2|E_I), \ldots, P(K_k|E_I)\},$$

які могли бути використані при формуванні криптограми E_I.

Множини апостеріорних ймовірностей утворюють апостеріорні знання противника про ключі $K=\{K_1, K_2, \ldots, K_k\}$ й повідомлення $M=\{M_1, M_2, \ldots, M_m\}$ після перехоплення криптограми E_I. Фактично, множини $P_{K|E_I}$ та $P_{M|E_I}$ становлять множини припущень, яким приписані відповідні ймовірності.

Основними показниками ефективності секретних систем прийнято вважати системи, які наведено нижче.

1. Криптографічна стійкість (кількість таємності), яку оцінюють як складність розв'язку задачі дешифрування перехопленого повідомлення (без знання ключа) найкращим відомим методом. Деякі криптосистеми спроектовано з таким розрахунком, що знання супротивника про її елементи не збільшуються в результаті перехоплення будь-якої кількості зашифрованих повідомлень. Інші системи, хоча й дають супротивникові деяку інформацію при перехопленні чергової криптограми, але не допускають єдиного розв'язку, тобто не дозволяють отримати однозначне розшифрування. Системи, що допускають єдиний розв'язок, дуже різноманітні як за витратою часу й сил, необхідних для одержання цього розв'язку, так і за кількістю матеріалу, який необхідно перехопити для його одержання.

2. Обсяг ключових даних. Симетрична система використовує загальний ключ для користувачів на передавальному та приймальному кінцях. Відповідно, цей ключ потрібно передати захищеним каналом зв'язку.

Отже, він не повинен бути занадто великим, щоб його можна було легко передати, і занадто малим, щоби його не можна було легко добути повним перебиранням множини ключів.

У випадку асиметричної криптосистеми один з ключів роблять загальнодоступним, отже, він передається відкритими каналами зв'язку.

3. Складність виконання прямого й зворотного криптографічного перетворення (шифрування і розшифрування повідомлень). Ці операції повинні бути по можливості простими і такими, що легко реалізуються на практиці.

4. Розростання кількості помилок. У деяких типах шифрів помилка в одній літері при шифруванні або передаванні призводить до великої кількості помилок при розшифруванні тексту, що може призвести до значної втрати інформації та навіть до повторного передавання інформації.

5. Збільшення обсягу повідомлення. У деяких типах секретних систем обсяг повідомлення збільшується в результаті операції шифрування. Часто такі шифри називають подрібнювальними. Цей небажаний ефект потрібно мінімізувати.

Однак, незалежно від того, який алгоритм використовує криптосистема,

симетричний чи асиметричний, вона повинна задовольняти такі вимоги:

– зашифрований текст можна прочитати лише за умови знання ключа розшифрування;

– трудомісткість обчислення криптографічного ключа шифрування за фрагментом криптограми та відповідним йому фрагментом відкритого тексту повинна бути занадто великою для її практичної реалізації;

– кількість операцій, необхідних для розшифрування інформації підбиранням ключа, повинна мати чітку нижню оцінку та виходити за межі можливостей сучасних комп'ютерних систем, а також мати достатній запас з урахуванням прогресу обчислювальної техніки;

– знання зловмисником алгоритму шифрування не повинно впливати на надійність системи захисту;

– незначна зміна ключа або відкритого тексту повинна призводити до суттєвої зміни зашифрованого тексту;

– в процесі шифрування необхідно забезпечувати постійний контроль за ключем шифрування та даними, що зашифровуються;

– довжина зашифрованого тексту не повинна бути набагато більшою довжини відкритого тексту;

– не повинно бути простих або таких, що легко встановити, залежностей між ключами, що послідовно використовуються в процесі шифрування;

– будь-який ключ з множини можливих повинен забезпечувати однаково надійний захист інформації;

– додаткові біти, що додаються до криптограми в процесі зашифрування, повинні бути повністю та надійно приховані в зашифрованому тексті;

– криптосистема повинна забезпечувати гарантовану швидкість шифрування за довільних параметрів відкритого тексту та ключів шифрування.

Криптосистеми можуть реалізовуватися як програмно, так і апаратно. Апаратна реалізація, без сумніву, має значно більшу вартість, однак і значні переваги, зокрема високу продуктивність, простоту використання, захищеність тощо. Програмна реалізація практичніше, гнучкіше у використанні, простіше модифікується.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні показники ефективності секретних систем.
2. Основні вимоги, які висуваються до сучасних криптосистем та їх класифікація.
3. Основні вимоги, які висуваються до симетричних криптосистем відносно їх безпеки. Класифікація симетричних криптосистем.

4. Основні вимоги, які висуваються до асиметричних криптосистем відносно їх безпеки. Класифікація асиметричних криптосистем.

5. Основні поняття теорії зв'язку в секретних системах.

6. Комбіновані криптосистеми: переваги та недоліки.

7. Основні математичні операції у побудові криптосистем.

8. Математична модель секретної системи.

9. Основні вимоги, які висуваються до забезпечення криптостійкості інформаційних систем.

Література: [1; 3; 4; 6; 10…17].

Тема 7. Алгоритми з секретним та відкритим ключами

План:

7.1 Стандарт DES

7.2 Основні модифікації DES та його основні режими роботи

7.3 Алгоритми криптографічних перетворень

7.4 Блокові та потокові шифри

7.5 Алгоритм RSA

7.6 Алгоритм Ель-Гамаля

7.1 Стандарт DES

Одним із найбільш відомим алгоритмом симетричного шифрування є DES (Data Encryption Standard – Стандарт Шифрування Даних). Цей алгоритм було розроблено у 1977 році, а в 1980 році було прийнято NIST (National Institute of Standards and Technolody США) у якості стандарту (FIPS PUB 46).

DES являє собою класичну сітку Фейстеля із двома множинами (рис. 7.1).

Дані шифрують 64-бітними блоками із використанням 56-бітного ключа. До секретних 56 бітів додають 8 бітів парності, тобто загальна довжина ключа дорівнює 64 біти.

Процес шифрування складається із чотирьох етапів. На першому виконують початкову перестановку (IP) 64-бітного вихідного тексту (забілювання), під час якої біти перемішуються відповідно до стандартної таблиці. Наступний етап складається із 16 раундів однієї і тієї ж функції, яка використовує операції зсуву й підстановки. На третьому етапі ліва і права половини виходу останньої (16-ї) ітерації міняються місцями. А на четвертому етапі – виконують перестановку IP^{-1} результату, який було отримано на третьому етапі (перестановка IP^{-1} обернена до початкової перестановки IP). На рисунку 7.2

наведено спосіб використання 56-бітного ключа.

Спочатку ключ подається на вхід функції перестановки. Потім для кожного із 16 раундів підключ K_i формується, як комбінація лівого циклічного зсуву та перестановки. Функція перестановки однакова для кожного раунду, але підключі K_i для кожного раунду отримують різними, внаслідок зсуву бітів ключа.

Рисунок 7.1 – Загальна схема DES

Шифрування (початкова перестановка). Початкова перестановка та її інверсія визначаються стандартною таблицею. Якщо M – це довільні 64 біти, то X=IP(M) – переставлені 64 біти. Якщо застосувати обернену функцію перестановки $Y=IP^{-1}(X)=IP^{-1}(IP(M))$, то вийде початкова послідовність бітів.

Стандартні таблиці IP та IP^{-1} наведено в таблиці 7.1 та 7.2 відповідно.

Таблиця 7.1 – Початкова IP-перестановка

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

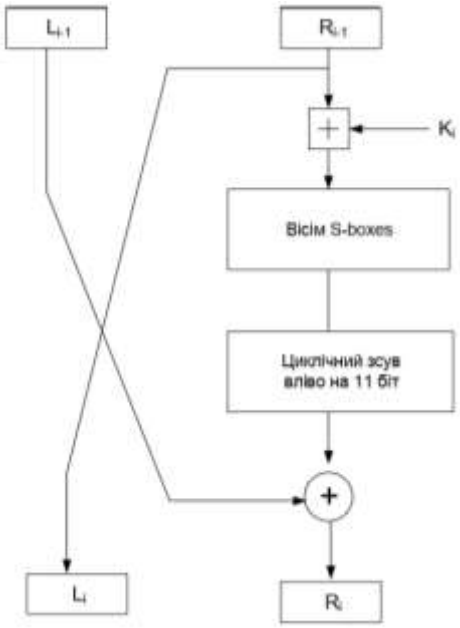

Рисунок 7.2 – Один раунд DES

Таблиця 7.2 – Кінцева IP^{-1}-перестановка

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Наведені таблиці необхідно читати таким чином: перший біт переставляють на 58-ме місце, другий – на 50-те тощо. Для оберненої перестановки: перший біт переставляють на 40-ве місце, другий – на 8-ме тощо.

Послідовність перетворень окремого раунду. Розглянемо послідовність перетворень, яку зазвичай використовують у кожному раунді. 64-бітний вхідний блок проходить через 16 раундів обробки, при цьому на кожній ітерації формується проміжне 64-бітне значення. Ліва і права частини кожного

проміжного значення трактуються як окремі 32-бітні значення, які позначають L і R. Кожна з ітерацій описується наступним чином:

$$L_i=R_{i-1}.$$

де $R_i=L_{i-1} \oplus F(R_{i-1}, K_i)$;

$\oplus$ – операція XOR (виняткова диз'юнкція (англ. eXclusive OR) – додавання за модулем).

Таким чином, вихід лівої половини L_i дорівнює входу правої половини R_{i-1}. Вихід правої половини R_i є результатом застосування операції XOR до L_{i-1} і функції F, що залежить від R_{i-1} та K_i.

Розглянемо функцію F докладніше. Блок R_i, який подається на вхід функції F, має довжину 32 біти. Спочатку R_i розширюється до 48 бітів, використовуючи таблицю, яка визначає перестановку і розширення на 16 бітів (табл. 7.3). Розширення відбувається у наступний спосіб: 32 біти розбиваються на групи по 4 біти, а потім розширюються до 6 бітів, приєднуючи крайні біти із двох сусідніх груп.

Таблиця 7.3 – Перестановка з розширенням

31	0	1	2	3	4
3	4	5	6	7	8
7	8	4	10	11	12
11	12	13	14	15	16
15	16	17	18	19	20
19	20	21	22	23	24
23	24	25	26	27	28
27	28	29	30	31	0

Читати таблицю необхідно так: на вхід перестановки подаються 32 біти тексту (біти пронумеровано від 0 до 31 – центральна частина табл. 7.3). До цих бітів додають додаткові біти (виділені стовпці у табл. 7.3) та отримують масив довжиною у 48 бітів.

У тексті розширення набуває такого вигляду: якщо частина вхідного повідомлення – ...efgh ijkl mnop..., то в результаті розширення отримуємо повідомлення – ...defghi hijklm lmnopq....

До отриманого в такий спосіб масиву бітів додається, за правилами XOR, 48-бітний раундовий ключ K_i. Результат подається на вхід блоку заміни, який складається із восьми S-боксів, тобто таблиць 4×16, в яких певним чином розміщено десяткові числа від нуля до п'ятнадцяти (у двійковому

представленні). Розміщення чисел було оптимізовано Агентством Національної Безпеки США під час розроблення стандарту для більшої стійкості алгоритму диференціального і лінійного криптоаналізу.

Підстановку здійснюють у такий спосіб. Масив у 48 бітів розбивається на вісім частин по шість бітів кожна. Кожну частину подають на «свій» S-бокс, номер якого визначається її номером. Перший і останній біт 6-бітової частини визначає номер рядка S-бокса у двійковому представленні, а чотири середні біти – номер стовпчика. На перетині рядка та стовпчика читаємо 4-бітове число. Воно і буде результатом заміни.

Операція розгортання ключа. Раундовий ключ формується за алгоритмом, який наведено нижче.

Крок 1. Із загального ключа шифрування вилучають кожен восьмий біт (під номерами: 8, 16, 24, 32, 40, 48, 56, 64 – біти парності). Довжина ключа таким чином зменшується до 56 бітів.

Крок 2. Біти ключа розділяються на два блоки C_0 і D_0 відповідно до стандартної таблиці PC-1 (Permuted Choice-1), яку наведено у таблиці 7.4.

Таблиця 7.4 – Таблиця перемішування бітів ключа PC-1

Блок C_0						Блок D_0							
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

Крок 3. На кожному і-му раунді C_i та D_i циклічно зсуваються вліво на 1 або 2 позиції, залежно від номера раунду (табл. 7.5).

Таблиця 7.5 – Параметри раундового зсуву регістрів C і D

Номер циклу	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Зсув вліво (шифрування)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
Зсув вправо (розшифрування)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Крок 4. Після зсуву підблоки C_i та D_i об'єднуються, а за допомогою функції PC-2 (Permuted Choice-2) вибирається 48 бітів раундового підключа K_i (табл. 7.6).

Вибір бітів відбувається наступним чином: підблоки розглядаються як послідовність рядків таблиці 7.4, які записуються один за одним, починаючи з першого. Біти отриманого таким чином блоку даних перенумеровуються зліва направо, починаючи із одиниці. Кожен елемент S таблиці прийнято розглядати

як номер біта b_S в отриманому блоці даних. Перетворенням є заміною усіх $S \rightarrow b_S$. Таким чином, блок-схема формування раундових ключів DES має наступний вигляд (рис. 7.3).

Таблиця 7.6 – Таблиця PC-2 для отримання раундового ключа DES

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

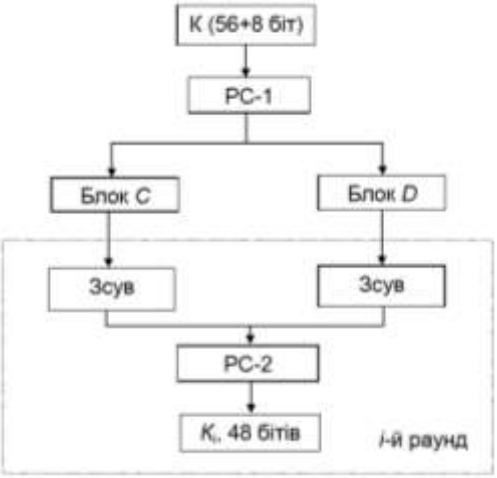

Рисунок 7.3 – Блок-схема формування раундових ключів DES

Операція розшифрування. Процес розшифрування аналогічний до процесу шифрування. На вхід алгоритму подають зашифрований текст, але ключі K_i використовуються в оберненій послідовності: K_{16} використовується на першому раунді, а K_1 – на останньому раунді.

Нехай виходом і-го раунду шифрування буде $L_i||R_i$. Тоді відповідний вхід 16-го раунду розшифрування буде $R_i||L_i$.

Після останнього раунду процесу розшифрування дві половини виходу міняються місцями так, щоб вхід заключної перестановки IP^{-1} був $R_{16}||L_{16}$. Виходом цієї стадії є незашифрований текст.

Перевіримо коректність процесу розшифрування. Використаємо зашифрований текст і ключ як вхідні параметри алгоритму. На першому кроці

виконаємо початкову перестановку IP і одержимо 64-бітне значення $Ld_0||Rd_0$. Відомо, що IP і IP^{-1} протилежні. Отже, $Ld_0||Rd_0=IP$ (зашифрований текст).

Зашифрований текст рівний $IP^{-1}(R_{16}||L_{16})$, тобто:

$$Ld_0||Rd_0=IP(IP^{-1}(R_{16}||L_{16}))=R_{16}||L_{16}.$$

Таким чином, вхід першого раунду процесу розшифрування еквівалентний 32-бітному виходу 16-го раунду процесу шифрування, у якого ліва і права частини записані у зворотному порядку.

Тепер необхідно показати, що вихід першого раунду процесу розшифрування еквівалентний 32-бітному входу 16-го раунду процесу шифрування.

По-перше, розглянемо процес шифрування:

$$L_{16}=R_{15};\ R_{16}=L_{15}\oplus F(R_{15}, K_{16}).$$

При розшифруванні:

$$Ld_1=Rd_0=L_{16}=R_{15};$$

$$Rd_1=Ld_0\oplus F(Rd_0, K_{16})=R_{16}\oplus F(Rd_0, K_{16})=(L_{15}\oplus F(R_{15}, K_{16}))\ \oplus F(R15, K16).$$

XOR зазвичай володіє наступними властивостями:

$$(A\oplus B)\ \oplus C=A\oplus\ (B\oplus C);$$

$$D\oplus D=0;\ E\oplus 0=E.$$

Таким чином, отримуємо $Ld_1=R_{15}$ і $Rd_1=L_{15}$. Отже, виходом першого раунду процесу розшифрування є $L_{15}||R_{15}$, який є наслідком перестановки входу 16-го раунду шифрування.

Легко довести, що ця відповідність виконується усі 16 раундів. Цей процес доцільно подати у загальних термінах, а для і-го раунду шифрувального алгоритму буде справедливо:

$$L_i=R_{i-1};\ R_i=L_{i-1}\oplus F(R_{i-1}, K_i).$$

Отримані рівності можна записати по-іншому:

$$R_{i-1}=L_i;\ L_{i-1}=R_i\oplus F(R_{i-1}, K_i)=R_i\oplus F(L_i, K_i).$$

Таким чином, описано входи і-го раунду як функція виходів.

Вихід останньої стадії процесу розшифрування є $R_0||L_0$. Щоб входом IP^{-1} стадії було $R_0||L_0$, необхідно поміняти місцями ліву і праву частини.

Але $IP^{-1}(R_0||L_0)=IP^{-1}$(IP (незашифрований текст))=незашифрований текст. Отже, одержуємо незашифрований текст, що і демонструє можливість розшифрування DES.

Переваги та недоліки DES. Через те, що довжина ключа рівна 56 біт, існує 2^{56} можливих ключів. На сьогодні така довжина ключа недостатня, оскільки допускає успішне застосування атак повного перебирання. Альтернативою DES можна вважати потрійний DES, IDEA, а також алгоритм Rijndael, прийнятий у

якості нового стандарту США на алгоритми симетричного шифрування.

Без відповіді поки залишається питання, чи можливий криптоаналіз алгоритму DES із використанням існуючих характеристик. Основою алгоритму є вісім таблиць підстановки, або S-бокси, які застосовуються в кожній ітерації. Існує небезпека, що ці S-бокси конструювалися таким чином, що криптоаналіз можливий лише для супротивника, який знає їх слабкі місця. Протягом багатьох років обговорювалася як стандартна, так і несподівана поведінка S-боксів, але все-таки нікому не вдалося виявити їх фатально слабкі місця. Більше того, коли Елі Біхам та Аді Шамір у 1990 році опублікували результати своїх досліджень з диференціального криптоаналізу, з'ясувалося, що блоки заміни DES значно стійкіші до цього типу криптоаналізу, ніж можна було очікувати при випадковому виборі їх структури. Це дозволяє стверджувати, що Агентству Національної Безпеки США цей тип атак на симетричні криптоалгоритми був відомий ще у 70-х роках XX сторіччя.

Перевагами цієї криптосистеми прийнято вважати:

– висока швидкодія як в апаратній, так і в програмній реалізації;

– можливість використання одних і тих самих апаратних або програмних блоків як для шифрування, так і для розшифрування інформації.

Основними недоліками DES є:

– невелика довжина ключа (усього 56 бітів);

– наявність «слабких» ключів, яка викликана тим, що для генерування ключової послідовності виконується два незалежних регістри зсуву;

– надмірність ключа, яка має біти контролю парності.

7.2 Основні модифікації DES та його основні режими роботи

Основним недоліком алгоритму DES є мала довжина ключа. В принципі, аналітики привернули увагу до цього питання відразу після виходу цього стандарту. Однак наприкінці 70-х років XX століття ще не існувало таких комп'ютерних потужностей, які б дозволили реалізувати атаку «грубою силою» (повного перебирання ключів). Проте, у 1998 році некомерційній правозахисній організації США Electronic Frontier Foundation з використанням спеціалізованого комп'ютера DES-cracker вдалося здійснити таку атаку за три дні.

Враховуючи це, відразу постало питання збільшення крипостійкості DES щодо атаки «грубою силою». Найбільш вдалими рішеннями прийнято вважати так званий «Потрійний DES» (Triple DES, 3DES) та DESX. Обидві модифікації дозволяють значно підсилити стійкість алгоритму до атак повного перебирання ключів.

Потрійний DES. На практиці існує багато різних варіантів потрійного DES. Найбільш популярними серед них є два: 3DES EDE2 (Encrypt-Decrypt-Encrypt з двома ключами) та 3DES EDE3 (Encrypt-Decrypt-Encrypt з трьома ключами).

Потрійний DES з двома ключами. У такому алгоритмі використовують два ключа по 56 біт, тобто загальна довжина ключа дорівнює 112 біт. Шифрування цим алгоритмом передбачає наступні етапи, які подано на рисунку 7.4.

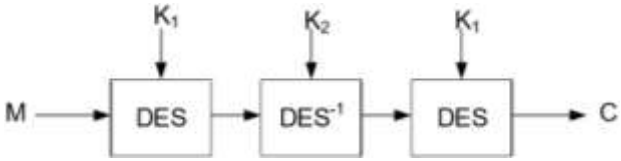

Рисунок 7.4 – Схема шифрування алгоритму 3DES EDE2

Як бачимо, відкрите повідомлення M спочатку шифрується звичайним однократним DES на ключі K_1, потім розшифровується на ключі K_2, після чого знов шифрується – на K_1. У цьому випадку зростання криптостійкості досягається за рахунок збільшення довжини загального ключа (до 112 біт + біти парності), так і кількості циклів обробки. На відміну від однократного, потрійний DES еквівалентний 48 раундам обробки відкритого тексту. Очевидно, що потрійний DES рівно втричі повільніший за звичайний, хоча і не такий повільний, як асиметричні алгоритми. Однак швидкий розвиток комп'ютерної техніки деякою мірою згладжує цей недолік. Етап розшифрування на ключі K_2 подано для сумісності з однократним DES у разі $K_1=K_2$.

Розшифрування відбувається протилежним чином: на вхід алгоритму подають зашифрований текст (C), на першому етапі розшифровують на ключі K_1, на другому – шифрують на K_2, на третьому – знов розшифровують на K_1. У результаті отримуємо розшифровану інформацію (M).

Потрійний DES з трьома ключами. Відмінність від попереднього алгоритму полягає в тому, що тут використовують три ключі шифрування, отже, стійкість системи до атаки «грубою силою» ще зростає. Загальна довжина ключа досягає 56×3=168 біт + біти парності. У випадку $K_1=K_2=K_3$ 3DES EDE3 перетворюється в однократний DES, що правда, втричі повільніший.

Схема шифрування за допомогою цього алгоритмом наведено на рисунку 7.5.

Розшифрування виконується аналогічно: спочатку шифроване повідомлення розшифровується на ключі K_3, потім зашифровується на ключі K_2, і, врешті решт, знов розшифровується, але на ключі K_1.

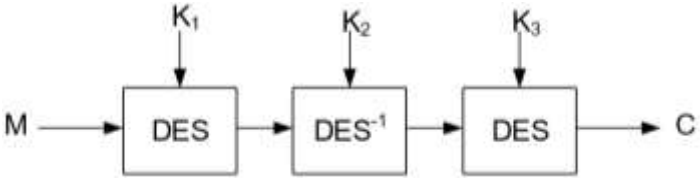

Рисунок 7.5 – Потрійний DES з трьома ключами

Падіння швидкодії під час роботі 3DES іноді дуже помітне, а у випадку режиму зчеплення блоків таке сповільнення не вдається компенсувати додатковим апаратним обладнанням. Для багатьох випадках, наприклад, під час шифрування критичних каналів зв'язку, таке падіння продуктивності є неприпустимим.

Алгоритм DESX. У 1984 році Роном Рівестом було запропоновано модифікацію DES, яка отримала назву DESX (DES eXtended), й була вільною від недоліків 3DES.

DESX визначається як:

$$DESX_{K1K2K3}=K_2 \oplus DES_K(K_1 \oplus M).$$

Як видно з наведеного виразу, повний ключ DESX складається із трьох: першого зашумлюючого K_1, який додається за правилами XOR до відкритого повідомлення; ключа DES K та іншого зашумлюючого ключа K_2, який додається за XOR до результатів шифрування DES.

Таким чином, загальна довжина ключа DESX становить 56+64+64=184 біта, що навіть більше, ніж у 3DES.

Що стосується збільшення часу обробки, то він усього на дві операції додавання XOR більший за звичайний DES.

Суттєвим для DESX є те, що цих дві операції додавання за модулем 2 (XOR) роблять шифр менш вразливим до атаки «грубою силою», проти чого і була спрямована ця розробка. DESX, однак, збільшує й стійкість простого DES проти диференціального та лінійного криптоаналізу, збільшуючи потрібну кількість проб із обраним відкритим текстом до 260.

Враховуючи це можна стверджувати, що DESX є кращим за DES. Цей алгоритм сумісний із DES, ефективно реалізується апаратно, може використовувати існуюче апаратне забезпечення DES.

7.3 Алгоритми криптографічних перетворень

Алгоритм криптографічного перетворення ГОСТ 28147-89. Даний стандарт шифрування даних було прийнято у 1989 році. В його основу було

покладено сітку Фейстеля. Параметри цього алгоритму наступні: довжина блоку – 64 біта; довжина ключа – 256 бітів; кількість раундів – 32.

Алгоритм є класичною сіткою Фейстеля:

$$L_i=R_{i-1};\ R_i=L_i \oplus F(R_{i-1}, K_i).$$

Функція F проста. Спочатку права половина та і-тий підключ додаються за модулем 2^{32}. Потім результат розбивається на вісім 4-ох бітових частин, кожна з яких надходить на вхід свого S-блока. ГОСТ 28147 використовує вісім різних S-блоків, кожний з яких має 4-ох бітовий вхід і 4-ох бітовий вихід. Виходи всіх S-блоків об'єднуються в 32-ох бітне слово, яке потім циклічно зсувається на 11 бітів вліво. Нарешті за допомогою XOR результат додається до лівої половини, у результаті чого виходить нова права половина (рис. 7.6).

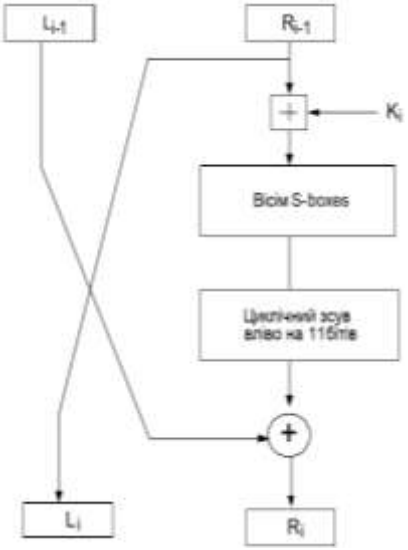

Рисунок 7.6 – Один раунд алгоритму ГОСТ 28147-89

Генерування ключів виконується дуже легко: 256-бітний ключ розбивається на вісім 32-ох бітних підключів. Алгоритм має 32 раунди, тому кожний підключ використовується у чотирьох раундах за схемою, яка наведена у таблиці 7.7, а S-блоки алгоритму – таблиця 7.8.

Вважається, що стійкість алгоритму ГОСТ 28147 багато в чому визначається структурою S-блоків. Довгий час їх структура у відкритій літературі не публікувалась. Входом і виходом S-блоків є 4-ох бітні числа, тому кожний S-блок може бути поданий у вигляді рядка чисел від 0 до 15,

розташованих у певному порядку. Заміна виконується у наступний спосіб: 32-ох бітний блок розбивається на вісім 4-ох бітних підблоків, кожен з яких подається на вхід свого блоку заміни. Номер S-box визначається порядковим номером 4-ох бітного підблоку. Двійкове значення, яке містить підблок, визначає номер комірки S-блоку, звідки треба взяти значення, яке і буде заміною.

Таблиця 7.7 – Використання підключів у ГОСТ 38147-89

Раунд	1	2	3	4	5	6	7	8
Підключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Підключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Підключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Підключ	8	7	6	5	4	3	2	1

Таблиця 7.8 – S-блоки алгоритму ГОСТ 28147-89

1-й S-блок	4	10	9	2	13	8	0	14
	6	11	1	12	7	15	5	3
2-й S-блок	14	11	4	12	6	13	15	10
	2	3	8	1	0	7	5	9
3-й S-блок	5	8	1	13	10	3	4	2
	14	15	12	7	6	0	9	11
4-й S-блок	7	13	10	1	0	8	9	15
	14	4	6	12	11	2	5	3
5-й S-блок	6	12	7	1	5	15	13	8
	4	10	9	14	0	3	11	2
6-й S-блок	4	11	10	0	7	2	1	13
	3	6	8	5	9	12	15	14
7-й S-блок	13	11	4	1	3	15	5	9
	0	10	14	7	6	8	2	12
8-й S-блок	1	15	13	0	5	7	10	4
	9	2	3	14	6	11	8	12

Основними відмінностями між DES і ГОСТ 28147 можна вважати наступне:

– DES використовує більш складну процедуру створення підключів, в порівнянні із ГОСТ 28147 (у ГОСТ ця процедура дуже проста: загальний 256-ох бітний ключ просто ділиться на вісім 32-ох бітних підключів);

– під час вибору сильних S-boxes ГОСТ 28147 вважається дуже стійким (у S-boxes DES 6-ти бітові входи й 4-ох бітові виходи, а в S-boxes ГОСТ 4-ох бітові входи й виходи; в обох алгоритмах використовується по вісім S-boxes, але розмір S-box ГОСТ суттєво менший за розміру S-box DES);

– у DES застосовуються нерегулярні перестановки P, а у ГОСТ використовується 11-ти бітний циклічний зсув вліво (перестановка DES збільшує лавинний ефект, коли зміна одного біту на вході призводить до зміни багатьох бітів на виході, а у ГОСТ зміна одного вхідного біта впливає на один S-box одного раунду, який потім впливає на два S-boxes наступного раунду, три S-boxes наступного тощо).

Таким чином, для того, щоби зміна одного біту на вході вплинула на кожен вихідний біт, DES вистачає 5 раундів, а ГОСТ для цього потрібно 8 раундів. Однак DES має 16 раундів, а ГОСТ – 32, що робить його більш стійким до диференціального і лінійного криптоаналізу.

У 2011 році з'явилися інформація про те, що за допомогою алгебраїчного криптоаналізу в ГОСТ 28147-89 було знайдено серйозні вразливості. До практичного застосування цього типу атак ще далеко, але безпека ГОСТ 28147-89 постраждала досить суттєво.

Алгоритм Rijndael. У 1997 році Національним Інститутом Стандартів і Технологій США (NIST) було оголошено про конкурс симетричних криптоалгоритмів на заміну DES, який вичерпав свої можливості в якості стандарту шифрування. У жовтні 2000 року було оголошено переможця цього конкурсу. Ним виявився алгоритм Rijndael (вимовляється – Рейндал), авторами якого були бельгійські криптографи Вінсент Реймен та Йоан Даймен. У листопаді 2001 року цей алгоритм був прийнятий як новий стандарт шифрування США під назвою AES (Advanced Encryption Standard – вдосконалений стандарт шифрування).

Одним із основних недоліків алгоритмів на основі сітки Фейстеля є те, що за один раунд шифрується лише половина вхідного блоку, а решта бітів просто переміщується без зміни в іншу половину. Як мінімум, це призводить до збільшення кількості раундів алгоритму.

Алгоритм Rijndael не належить до фейстелівських. Замість цього раундова функція складається із чотирьох різних перетворень, які називаються шарами, і обробляють весь вхідний блок разом.

Кожний шар розроблявся з урахуванням протидії лінійному та диференціальному криптоаналізу. В основу кожного шару покладена своя власна функція.

1. Нелінійний шар складається із паралельного застосування S-блоків для оптимізації нелінійних властивостей.

2. Шар лінійного переміщення рядків гарантує високий степінь дифузії для невеликої кількості раундів.

3. Шар лінійного переміщення стовпців також гарантує високий степінь дифузії для невеликої кількості раундів.

4. Додатковий шар підмішування ключа складається з простого XOR проміжного стану із ключем раунду.

Перед першим раундом застосовується додаткове забілювання з використанням ключа. Причина цього полягає в тому, що будь-який шар після останнього або до першого додавання ключа може бути просто знятий без знання ключа і тим самим не додає безпеки в алгоритм (наприклад, початкова і кінцева перестановки в DES).

Початкове або кінцеве додавання ключа застосовується також у деяких інших алгоритмах, наприклад, IDEA, SAFER і Blowfish. Для спрощення структури алгоритму шар лінійного переміщення останнього раунду відрізняється від шару переміщення інших раундів. Можна показати, що це в жодному разі не підвищує і не знижує безпеку аналогічно відсутності операції swap в останньому раунді DES.

Шифр є послідовністю ітерацій, які виконуються над деякою проміжною структурою, яка називається станом. Стан може бути представлений у вигляді прямокутного масиву байтів. Масив має чотири рядка, а кількість стовпчиків, яку позначають N_b, дорівнює довжині блока, поділеній на 32.

Ключ шифрування аналогічно подається у вигляді прямокутного масиву байтів з чотирьох рядків. Кількість стовпчиків (N_k) визначається довжиною ключа також поділеною на 32. Вхідні та вихідні дані подаються як одновимірні масиви байтів відповідної довжини.

Стан і ключовий масив заповнюються з цих масивів спочатку за стовпчиками, а потім за рядками так, як наведено у таблиці 7.9.

Кількість раундів N_r залежить від N_b та N_k відповідно до таблиці 7.10.

Раундова функція складається з чотирьох перетворень:

– застосування таблиці заміни (ByteSub);
– зсуву рядків (ShiftRow);
– перемішування стовпчиків (MixColumn);
– підмішування раундового ключа (AddRoundKey).

Останній раунд відрізняється від усіх попередніх, тим що він не використовує перемішування стовпчиків. Зауважимо, що на відміну від

фейстелевських алгоритмів, раундова функція діє на весь вхідний блок разом.

Таблиця 7.9 – Порядок байтів у стані

0	4	8	12	…
1	5	9	13	…
2	6	10	14	…
3	7	11	15	…

Таблиця 7.10 – Кількість раундів як функція довжин блоку і ключа

Nr	N_b=4 (128 біт)	N_b=6 (192 біти)	N_b=8 (256 біт)
N_k=4 (128 біт)	10	12	14
N_k=6 (192 біти)	12	12	14
N_k=8 (256 біт)	14	14	14

Блок-схема процесу шифрування алгоритму AES подано на рисунку 7.7.

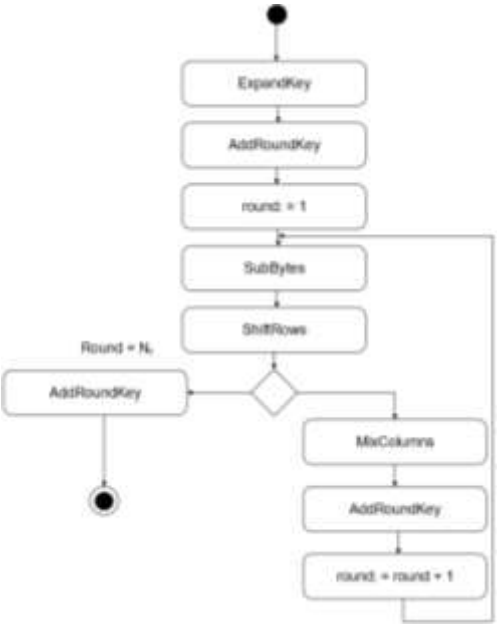

Рисунок 7.7 – Блок-схема процесу шифрування алгоритму AES

Опишемо окремі перетворення раундової функції.

1. Перетворення SubBytes. Суть цього перетворення полягає в заміні кожного байта {xy} стану (де x та y – шістнадцяткові значення) на інші

відповідно до таблиці заміни, яку наведено на рисунку 7.8. Зрозуміло, що під час розшифрування необхідно використати обернену таблицю, яка подана на рисунку 7.9. Наприклад, байт {fe} за таблицею на рисунку 7.8 буде замінено на {bb}, а байт {bb} за таблицею на рисунку 7.9 – на {fe}, що і свідчить про взаємну оберненість таблиць заміни.

З математичної точки зору заміна еквівалентна таким операціям в полі Галуа $GF(2^8)$, яке використовується в цьому алгоритмі:

– кожний байт замінюють на обернений елемент за операцією множення, визначеній в цьому полі ({00} відображується сам на себе);

– потім застосовується афінне перетворення, яке визначається за наступним виразом (множення та додавання виконується за правилами, визначеними в полі Галуа $GF(2^8)$):

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \times \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

2. ShiftRows (зсув рядків). Суть цього перетворення полягає у циклічному зсуві рядків стану. Схематично такий зсув подано на рисунку 7.10.

Перший рядок залишається незмінним. Другий – зсувається вліво на один байт, а перший байт записується в кінець рядка. Третій зсувається на два байти, а четвертий – на три. Обернене перетворення – зсув вправо.

3. Перетворення MixColumns. Це перетворення виконується як множення квадратної матриці четвертого порядку на кожен стовпчик стану:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

По суті, це означає, що стовпчики стану розглядаються як поліноми в $GF(2^8)$ і множаться за модулем x^4+1 на фіксований поліном (коефіцієнти даються у 16-ковій формі):

$$c(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}.$$

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рисунок 7.8 – Таблиця заміни для шифрування алгоритму Rijndael

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Рисунок 7.9 – Обернена таблиця заміни для процесу розшифрування

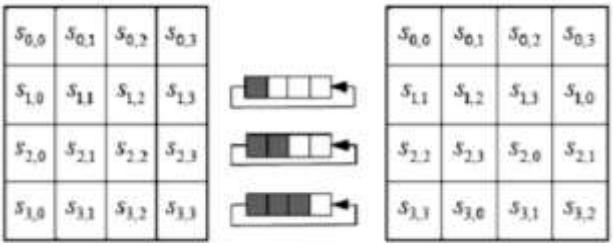

Рисунок 9.10 – Перетворення ShiftRows

Цей поліном взаємно простий з x^4+1 і, отже, існує обернений до нього поліном. Інверсія MixColumn визначається таким чином:

$$(\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}) \oplus d(x)=\{01\}.$$

Добуток виконується за правилами поля Галуа $GF(2^8)$. У результаті отримаємо:

$$d(x)=\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\}.$$

У матричному вигляді будемо мати обернену операцію до MixColumn, яка використовується при розшифруванні:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

Тут множення також відбувається за правилами $GF(2^8)$.

4. Перетворення AddRoundKey. Дане перетворення зводиться до побітового додавання за модулем два (XOR) кожного біта раундового ключа з бітами стану. Оберненим перетвореннv до AddRoundKey служить воно саме.

5. Процедура ExpandKey. Ця процедура приймає на вході ключ шифрування і перетворює його на ключі для усіх раундів. Загальна кількість бітів ключового масиву дорівнює довжині блоку, помноженій на кількість раундів плюс 1, тобто $N_b \times (N_r+1)$. Наприклад, для довжини блоку 128 бітів і 10 раундів необхідно 1408 бітів ключового масиву.

Операція розгортання ключа виконується в такий спосіб. Перші N_k позицій розширеного ключа заповнюються ключем шифрування. Наступні 4-ох байтні слова, w[i], утворюються як результат операції XOR між w[i-1] та w[i-N_k] словами. Для слів, позиція яких кратна N_k, додатково перед XOR'ом до w[i-1] застосовується трансформація, яка складається з циклічного зсуву байтів у слові, додавання за правилами XOR з константою раунду $R_{con}[i]$ та виконання табличної підстановки для усіх байтів слова. Слід зазначити, що операція розгортання ключа має два варіанти: для $N_k \leq 6$ та $N_k > 6$ (відмінність для $N_k > 6$ полягає в тому, що таблична підстановка виконується до XOR з $R_{con}[i]$).

Константи раунду не залежать від N_k і визначаються в такий спосіб:

$$R_{con}[i]=(\{02^{i-1}\}, \{00\}, \{00\}, \{00\}).$$

Раундові ключі вибираються з ключового масиву від w[$N_b \times i$] до w[$N_b \times (i+1)$].

На рисунку 7.11 подано алгоритм розшифрування. Як бачимо, усі перетворення виконуються в оберненому порядку. Замість шифрувальних

перетворень використовуються розшифрувальні.

1. InvSubBytes – операція заміни байтів, яка використовує обернену таблицю заміни.

2. InvShiftRows – циклічний зсув байтів вправо, протилежно до такого при шифруванні.

3. InvMixColumns – перемішування стовпчиків з використанням оберненої матриці.

4. Процедури ExpandKey та AddRoundKey залишаються без змін.

5. Раундові ключі для розшифрування використовуються в оберненому порядку.

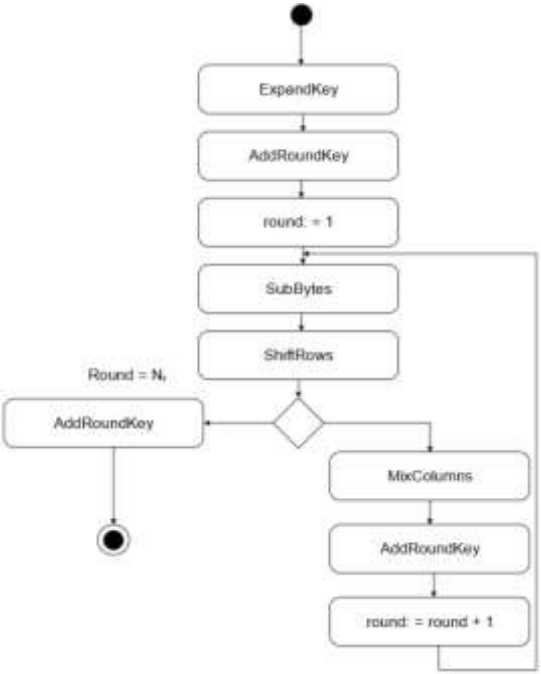

Рисунок 7.11 – Алгоритм розшифрування Rijndael

Переваги та недоліки алгоритму Rijndael. За оцінками розробників цей алгоритм уже на чотирьох раундах має криптостійкість, яка є достатньою для сучасних застосувань. Теоретичною межею вважаються 6…8 раундів. Отже, 10…14 раундів, які пропонують розробники, мають значний запас криптостійкості.

Переваги, які відносяться до аспектів реалізації наведено нижче.

1. Rijndael може виконуватись швидше, ніж традиційний блоковий алгоритм шифрування на основі сітки Фейстеля, оскільки розробниками проведено оптимізацію між розміром таблиці і швидкістю виконання.

2. Rijndael придатний для реалізації в смарт-картах, оскільки він може працювати з невеликим RAM (англ. Random Access Memory – пам'ять з довільним доступом) і є невелику кількість раундів.

3. Раундові перетворення добре розпаралелюються, що є важливою перевагою для майбутніх процесорів і спеціалізованої апаратури.

4. Алгоритм шифрування не використовує арифметичні операції, тому тип архітектури процесора не має значення.

5. Алгоритм шифрування повністю самодостатній та не використовує ніяких інших криптографічних компонентів, S-boxів, взятих з добре відомих алгоритмів, бітів, отриманих зі спеціальних таблиць.

6. Безпека алгоритму не базується на ітераціях арифметичних операцій, які складно зрозуміти, проста розробка краще аналізується, і крім того, в компактній структурі практично неможливо приховати «люки» або дефекти.

Структура алгоритму дозволяє використовувати шифр з різними довжинами блоку, від 128 до 256 бітів з кроком в 32 біти. Окрім того, операція розгортання ключа може працювати з ключами, довжина яких кратні 4 байтам. Для іншої довжини ключа необхідно знати лише кількість раундів алгоритму, яка визначається з наступного виразу:

$$N_r=\max(N_k, N_b)+6.$$

Таким чином, цей алгоритм є надзвичайно гнучким, а його криптостійкість можна змінювати залежно від ситуації, налаштовуючи її зміною довжини ключа, блоку та кількістю раундів.

Відносним його недоліком можна вважати те, що його структура є недостатньо вивченою, а отже, містить невідомі зараз недоліки.

7.4 Блокові та потокові шифри

Алгоритм RC2. Криптоалгоритм RC2 є блоковим шифром із ключем змінної довжини, розроблений Р. Рівестом на замовлення компанії RSA Data Security, Inc. Абревіатура «RC» означає Ron's Code (Код Рональда), або Rivest's Cipher (Шифр Рівеста).

Криптоалгоритм розроблявся як альтернатива стандарту DES. RC2 працює із блоками по 64 біти, програмна реалізація криптоалгоритму приблизно у два-три рази швидша, ніж DES. Змінна довжина ключа дозволяє домогтися адекватної криптостійкості з урахуванням можливостей силової атаки.

Уряд США не забороняє експортувати апаратні і програмні реалізації криптоалгоритмів RC2 і RC4 – при дотриманні 40-бітового обмеження на довжину ключа. Американські компанії за межами США і Канади можуть використовувати крипто-алгоритми з довжиною ключа 65 бітів.

При шифруванні за криптоалгоритмом RC2 до секретного ключа методом конкатенації додається деякий допоміжний ключ від 40 до 88 бітів. Для виконання дешифрування допоміжний ключ передається одержувачу зашифрованого повідомлення у відкритому вигляді.

Алгоритм RC5. Криптоалгоритм RC5 також розроблений Р. Рівестом на замовлення компанії RSA Data Security, Inc. Це блоковий шифр зі змінною довжиною блоку (32, 64 і 128 бітів), ключа і кількістю циклів криптографічного перетворення (від 0 до 255). Довжина ключа варіюється від 0 до 2048 бітів. Така параметризація дозволяє гнучко налаштувати криптоалгоритм із урахуванням конкретних вимог до криптостійкості та ефективності реалізації.

Криптоалгоритм RC5 складається із трьох основних процедур: розгортання ключа, шифрування і розшифрування. У процедурі розгортання ключа заданий секретний ключ піддається спеціальному перетворенню з метою заповнення ключової таблиці, причому розмір таблиці залежить від кількості циклів криптографічного перетворення. Ключова таблиця використовується потім для шифрування і розшифрування. Процедура шифрування складається із трьох основних операцій: цілочисельного сумування, додавання за модулем 2 і циклічного зсуву.

Безумовна перевага криптоалгоритму полягає у простоті реалізації. Непередбачуваність результату операції циклічного зсуву, що залежить від конкретних вхідних даних при шифруванні, забезпечує необхідний рівень криптостійкості. Дослідження криптостійкості RC5 показали, що варіант криптоалгоритму з розрядністю блоку 64 біти та 12 (і більше) циклами перетворення гарантує адекватну криптостійкість до диференціального та лінійного криптоаналізу.

Алгоритм IDEA. IDEA (International Data Encryption Algorithm) є блоковим симетричним алгоритмом шифрування, розробленим Сюдзя Лай (Xuejia Lai) і Джеймсом Мессі (James Massey) зі швейцарського федерального інституту технологій. Перша версія була опублікована у 1990 році. Переглянута версія алгоритму, посилена засобами захисту від диференціальних криптографічних атак, була подана в 1991 р. і докладно описана в 1992 р.

IDEA претендував на роль одного з симетричних алгоритмів, якими передбачалось замінити DES.

Алгоритм SAFER. Криптоалгоритм SAFER (Secure And Fast Encryption Routine) є блоковим шифром, розробленим на замовлення корпорації Cylink.

Довжина ключа шифрування в одній з версій дорівнює 64 біти. Криптоалгоритм орієнтований на байтову обробку блоків по 64 біти, і має змінну кількість раундів криптографічного перетворення (для описаної специфікації – 6).

Цей шифр, на відміну від більшості блокових шифрів, має різні процедури шифрування і розшифрування. Перша версія SAFER з довжиною ключа 64 біти відома за назвою SAFER K-64. Друга версія – SAFER K-128 має 128-бітний ключ.

Результати криптоаналізу продемонстрували криптостійкість SAFER K-64 стосовно диференціаль-ного та лінійного криптоаналізів при дотриманні однієї умови – кількість циклів перетворення повинна бути більше шести. У результаті досліджень було виявлено слабке місце процедури перетворення ключа. У нових модифікаціях SAFER SK-64 і SAFER SK-128 виявлений недолік усунутий.

Алгоритм FEAL. Криптоалгоритм FEAL був розроблений як альтернатива DES. Оригінальний криптоалгоритм (FEAL-4) був розрахований на програмну реалізацію і мав чотири цикли перетворення при обробці 64-бітного блоку та 64-бітного ключа шифрування. Криптоаналітичне дослідження продемонструвало слабкість криптоалгоритму – для розкриття ключа при атаці на основі обраного відкритого тексту досить 20 зразків.

Успіхи в криптоаналізі FEAL-8 (вісім циклів перетворення) призвели до появи модифікації зі змінною кількістю циклів перетворення FEAL-N. Опубліковані результати успішного диференціального криптоаналізу FEAL-N при $N \leq 31$. Для розкриття ключа FEAL-8 методом лінійного криптоаналізу досить 225 різних відкритих текстів.

Алгоритм Blowfish. Алгоритм Blowfish є 16-раундовою сіткою Фейстеля з довжиною блоку в 64 біти. Ключ може мати довільну довжину в межах 448 бітів. Хоча перед початком шифрування виконується складна фаза ініціалізації, саме шифрування даних виконується досить швидко. Алгоритм призначений, в основному для застосувань, де ключ міняється нечасто, до того ж існує фаза початкової автентифікації сторін, під час якої відбувається узгодження загальних параметрів шифрування.

Під час реалізації на 32-бітних мікропроцесорах з великим кешем даних Blowfish значно швидше DES.

Алгоритм складається із двох частин: розгортання ключа і шифрування даних. Розгортання ключа перетворює ключ довжиною, принаймні 448 бітів, у

кілька масивів підключів загальною довжиною 4168 байтів. Кожний раунд шифру складається з перестановки, залежної від ключа, і заміни, яка залежить, і від ключа, і від даних. Раундовими операціями є XOR і додавання 32-бітних слів.

Алгоритм RSB-32. Алгоритм RSB-32 (назва походить від англійських слів Round, Step, Block – Раунд, Крок, Блок) – ітераційний блоковий шифр зі змінними довжинами ключа, блоку та елементів блоків, над якими виконуються нелінійні операції заміни. На відміну від інших симетричних шифрів у RSB таблиці заміни змінюються залежно від стану секретного ключа. Алгебраїчні перетворення у RSB виконуються над кільцем лишків за деяким модулем m. Загальні параметри шифру такі:

– довжина раундового ключа – 32 біти;
– довжина загального (крокового) ключа: r×64, r=1, 2, ...;
– кількість кроків шифрування: s=1, 2, ...;
– кількість раундів шифрування:r×s;
– розмір блоку: 256, 512, 1024 біти;
– розмір елементів заміни: 8, 16, або 32 біти (RSB – криптосистема, орієнтована на роботу з 8- ,16-, або 32-розрядними процесорами).

Загальний ключ (Common Key) у RSB-шифрі утворюється конкатенацією r 32-розрядних раундових ключів (Round Key).

Алгоритм «Мухомор». В основу алгоритму «Мухомор» покладено математичні та структурні ідеї схеми Лая-Мессі, який також використовує деякі ідеї, які реалізовано в шифрі IDEA NXT. Але у цьому шифрі, порівняно із IDEA NXT, використано ефективніші як з точки зору стійкості, так і з точки зору продуктивності, оригінальні базові криптографічні алгоритми – функції ускладнення базових перетворень M-64, M-128 та M-256, розширено параметри для більших довжин блоків та ключів, запропоновано відповідні реалізації, а також удосконалено схеми розгортання підключів. Усе це дозволяє уникати низки потенційних вразливостей та підвищити продуктивність шифру для апаратної, програмної та апаратно-програмної реалізацій.

Алгоритм ADE. Основну увагу під час розроблення ADE приділялося можливості динамічного керування процесом лінійного розсіювання й нелінійної заміни в ході криптографічного перетворення інформації. З цією метою в базову структуру алгоритму AES введено блоки (криптопримітиви) лінійного розсіювання й нелінійних замін, що динамічно змінюються, а правила функціонування їх задаються значеннями раундових ключів.

Властивості введених примітивів криптоалгоритму ADE не поступаються

криптопримітивам алгоритму AES, а за рахунок їх динамічної зміни на кожному раунді ітеративної обробки вдається динамічно керувати процесом перетворення інформації. Це, з одного боку, не погіршує (порівняно з AES) стійкість ADE до відомих методів криптоаналізу, з іншого боку, істотно ускладнює процес формування алгебраїчних рівнянь, що аналітично зв'язують стан відкритого тексту, шифротексту і ключа.

Алгоритм «Калина». Алгоритм «Калина» подібний до Rijndael, однак він має деякі вдосконалення з метою збільшення криптостійкості.

Основні відмінності «Калини» від Rijndael полягають у наступному:

– збільшена кількість циклів шифрування; використано додавання за модулем 2^{32} і за модулем 2 для введення ключової інформації для покращення захисту від алгебраїчних атак, лінійного та диференціального криптоаналізів, інтерполяційної атаки тощо;

– використано 8 блоків нелінійного перетворення (S-блоків) замість одного для додаткового захисту від алгебраїчних атак, покращення властивостей розсіювання шифру;

– використання випадково сформованих S-блоків, відібраних за критеріями стійкості до диференціального, лінійного криптоаналізу та степені нелінійності булевих функцій;

– принципово нова схема розгортання ключа для захисту від всіх відомих атак на схеми вироблення підключів; досить висока продуктивність.

Усі модифікації спрямовані на збільшення стійкості та перекриття потенційних вразливостей Rijndael, що виявлено останніми роками.

Алгоритм «Лабіринт». Алгоритм «Лабіринт» є ітеративним шифром, тобто основу його процедури шифрування становить циклове перетворення, що повторюється задану кількість разів (позначимо число циклів шифрування символом r). Кожен цикл складається із двох абсолютно ідентичних ітерацій, однак, з огляду на те, що для шифрування одного блоку потрібно, як мінімум, дві ітерації, поняття циклу не співпадає з поняттям ітерації.

Окрім циклового перетворення процедура шифрування включає початкове (IT) і кінцеве (FT) перетворення. Властивість інволютивності шифру досягається за рахунок застосування класичної конструкції напівблокової сітки Фейстеля.

Алгоритм «Лабіринт», незалежно від довжини блоку й ключа, використовує фіксовану кількість ітерацій шифрування – 16 (інакше кажучи, 8 циклів – r=8).

7.5 Алгоритм RSA

Не дивлячись на досить велику кількість різних асиметричних

криптосистем, широке практичне застосування отримала RSA, назва якої походить від перших літер прізвищ її авторів: Рональда Рівеста (Ron Rivest), Аді Шаміра (Adi Shamir) та Леонарда Аделмана (Leonard Addleman).

Криптосистема RSA використовує односторонню функцію утворення добутку двох великих простих цілих чисел, що значно простіше, ніж розкладання такого великого цілого числа на прості множники. Зрозуміло, що це принципово можна зробити, однак, витрати ресурсів (часу або обчислювальної потужності комп'ютерів) будуть не меншими, ніж просте суцільне перебирання усього ключового масиву.

Звичайно, що наявність гарантованої оцінки криптостійкості алгоритму створила сприятливі умови для розповсюдження криптосистеми RSA на фоні інших алгоритмів. Це й стало однією із причин її популярності у банківських системах для роботи з віддаленими клієнтами.

Розглянемо алгоритм шифрування за схемою RSA. Зазвичай, із навчальною метою використовуються приклади із малими числами, однак для реальної роботи ці числа не підходять, оскільки криптостійкість такої системи практично дорівнює нулю.

Алгоритм RSA є блоковим алгоритмом, де даними є цілі числа з відрізку [0, n-1] для деякого n.

Отже, для обміну інформацією, зашифрованою за допомогою криптосистеми RSA, виконують нижче перераховані кроки.

Крок 1. Підготовчі обчислення. Отримувач генерує два великих простих числа p і q (мінімум 128-бітних). Для прикладу візьмемо p=7 й q=11. Обчислимо добуток, модуль криптосистеми, $n=p\times q=77$. Далі необхідно обчислити функцію Ейлера для цього модуля. Відомо, що для простих чисел $\varphi(n)=(p-1)(q-1)$. Отже, $\varphi(77)=6\times10=60$. Тепер необхідно згенерувати ціле число, воно має бути взаємно простим, як з n, так і з $\varphi(n)$, наприклад, e=13.

Пара чисел (e, n) буде формувати публічний ключ криптосистеми. У нашому випадку це буде пара (13, 77).

Тепер необхідно обчислити приватний ключ d, парний до обраного публічного. Для цього треба розв'язати рівняння: $(d\times e) \bmod \varphi(n)=1$. Відповідно до обчислень мультиплікативного оберненого, будемо мати: $d=(1+k\times\varphi(n))/e$, де k – ціле число. Оскільки приклад дуже простий, то простим перебиранням для k=8 отримуємо d=37. Отже, приватним ключем, парним до нашого публічного (13, 77) буде служити пара чисел (d, n) – (37, 77).

Крок 2. Розповсюдження ключів. Для шифрування інформації використовують публічний ключ (хоча можна використовувати і приватний,

деякі асиметричні криптосистеми, в тому числі RSA, це дозволяють). Для використання його розміщують на ресурсі, до якого мають доступ усі учасники інформаційного обміну. Зауважимо, що одним публічним ключем можуть користуватися усі, хто бажає обмінюватися з отримувачем зашифрованою інформацією. На відміну від симетричних криптосистем, тут немає необхідності для кожної пари учасників генерувати окрему пару ключів, адже розшифрувати інформацію за допомогою публічного ключа неможливо (в усякому разі, обчислювати складно).

Для простого прикладу необхідно в подальшому продемонструвати атаку перешифруванням, коли багаторазове шифрування перехопленого повідомлення призводить до відкритого тексту. Тут йдеться лише про те, щоб трудомісткість такої атаки була не меншою, ніж трудомісткість атаки безпосереднього перебирання ключів. Таким чином, конфіденційність обміну інформації гарантується самим принципом обробки інформації. Єдине, що необхідно зробити, це захистити публічний ключ від підміни (про атаки на асиметричні криптосистеми наведено далі). Найпростіше, що можна зробити, це захистити каталог, де знаходяться ключі, від запису, однак найнадійнішим способом вважається сертифікація публічних ключів. Кожен, хто бажає захистити свій публічний ключ від підміни, повинен отримати сертифікат довірчого центру інфраструктури відкритих ключів, який прив'язує ключ до його власника.

Приватний ключ не розповсюджується. Він використовується для розшифрування інформації та створення електронного цифрового підпису, і повинен бути відомим лише його власникові.

На цьому підготовчі операції закінчено, і можна починати обмін захищеною інформацією.

Крок 3. Шифрування інформації. Криптосистемою RSA можна зашифрувати числа (десяткові коди літер) у діапазоні від 0 до n. Відправник повідомлення, використовуючи публічний ключ (e, n), у нашому випадку – (13, 77), за допомогою виразу $C_i=(M_i)^e \bmod n$ зашифровує своє повідомлення, де M_i – числове подання чергової літери повідомлення, C_i – черговий символ криптограми.

Наприклад, слово «БАНК» (яке має числове представлення «02 01 17 14» за таблицею заміни української абетки алфавіту, яка починається з 01) зашифрується таким чином:

$$C_1=2^{13} \bmod 77=30;$$
$$C_2=1^{13} \bmod 77=1;$$
$$C_3=17^{13} \bmod 77=73;$$

$$C_4=14^{13} \bmod 77=49.$$

Отже, криптограма буде мати вигляд: «30 01 73 49». Очевидно, що шифр в нашому прикладі є шифром простої заміни. Як бачимо, літера «А», яка має код «01», не змінилася. Таку ж властивість мають «0» та n-1. Отже, не всі числа доцільно вибирати в якості кодів літер. Вважається правильним надавати для шифрування числа з діапазону [2, n-2]. Це дещо ускладнює розкриття шифру.

Зашифрований текст пересилається отримувачу відкритими каналами зв'язку.

З наведеного способу шифрування може скластися враження, що піднесення великого цілого числа у великий степінь та взяття залишку за модулем третього великого числа є надзвичайно складною математичною задачею. Однак насправді це зовсім не так. Для ілюстрації цього наведемо алгоритм обчислення виразу $432^{678} \bmod 987$.

Число 678 можна подати у наступному вигляді: 678=512+128+32+4+2. Тоді:

$$432^{678} \bmod 987=(432^{512}\times 432^{128}\times 432^{32}\times 432^{4}\times 4322) \bmod 987.$$

Враховуючи основні властивості отримуємо:

$$432^{678} \bmod 987=((432^{2} \bmod 987)\times(4324 \bmod 987)\times(432^{32} \bmod 987)\times$$
$$\times (432128 \bmod 987) \times(432^{512} \bmod 987)) \bmod 987.$$

Тепер необхідно обчислити ступені числа 432:

$$432^{2}\times \bmod 987=81;$$
$$432^{4}\times \bmod 987=81^{2}\times \bmod 987=639;$$
$$432^{8}\times \bmod 987=639^{2}\times \bmod 987=690;$$
$$432^{16}\times \bmod 987=690^{2}\times \bmod 987=366;$$
$$432^{32}\times \bmod 987=366^{2}\times \bmod 987=711;$$
$$432^{64}\times \bmod 987=711^{2}\times \bmod 987=177;$$
$$432^{128}\times \bmod 987=177^{2}\times \bmod 987=732;$$
$$432^{256}\times \bmod 987=732^{2}\times \bmod 987=870;$$
$$432^{512}\times \bmod 987=870^{2}\times \bmod 987=858.$$

Підставляючи у вираз ці значення, отримаємо:

$$(81\times 639\times 711\times 732\times 858) \bmod 987=204.$$

Крок 4. Розшифрування інформації. Отримувач розшифровує зашифроване повідомлення «30 01 73 49», використавши тільки йому відомий приватний ключ (d, n) та формулу $M_i=(C_i)^d \bmod n$.

Доведемо принципову можливість розшифрування зашифрованої на публічному ключі інформації:

$$(C)^d \bmod n=(M^e \bmod n)^d \bmod n=(M_e)^d \bmod n=(M^{ed}) \bmod n=(M^{1+k\varphi(n)}) \bmod n=$$
$$=M(M^{\varphi(n)}) \bmod n=M.$$

Таким чином, операція шифрування на публічному та розшифрування на приватному ключі – взаємно зворотні.

У цьому випадку приватним ключем служить пара (37, 77). Тоді отримаємо:

$$M_1=30^{37} \bmod 77=2;$$
$$M_2=1^{37} \bmod 77=1;$$
$$M_3=73^{37} \bmod 77=17;$$
$$M_4=49^{37} \bmod 77=14.$$

Маючи таблицю заміни, за кодами літер отримаємо «БАНК».

Отже, визначено методи шифрування та розшифрування інформації у криптосистемі RSA. Залишилося вияснити один цікавий факт, характерний для цієї криптосистеми: чи дозволить вона шифрувати інформацію приватним ключем, а розшифровувати – публічним?

Нехай повідомлення для шифрування таке ж саме: «БАНК» або «02 01 17 142. Зашифруємо її на приватному ключі (37, 77). Отримаємо таке:

$$C_1=2^{37} \bmod 77=51;$$
$$C_2=1^{37} \bmod 77=1;$$
$$C_3=17^{37} \bmod 77=52;$$
$$C_4=14^{37} \bmod 77=42.$$

Тепер розшифруємо зашифроване повідомлення «51 01 52 42» на публічному ключі (13, 77):

$$M_1=51^{13} \bmod 77=2;$$
$$M_2=1^{13} \bmod 77=1;$$
$$M_3=52^{13} \bmod 77=17;$$
$$M_4=42^{13} \bmod 77=14.$$

Як бачимо, отримане відкрите повідомлення «БАНК» і таким методом.

Отже, криптосистема RSA симетрична відносно застосування парних ключів: можна зашифровувати інформацію на публічному ключі та розшифровувати на приватному і навпаки, зашифровувати на приватному, а розшифровувати – на парному до нього публічному ключі.

Безпека та швидкодія RSA. Швидкодія апаратної реалізації RSA приблизно в 1000 разів нижча, ніж реалізації DES. Наприклад, швидкодія реалізації RSA з 512-бітовим модулем – 64 Кбіт/с. На сьогодні розробляються мікросхеми з 512-бітовим модулем, швидкодія яких прямує до 1Мб/с. Існують також мікросхеми RSA, які оперують із 1024-бітовими числами, але вони вкрай повільні. Виробники також реалізують RSA в інтелектуальних картках, однак продуктивність цих реалізацій невисока.

Що стосується програмних реалізацій, то наприклад, програмна реалізація

DES приблизно в 100 разів швидша програмної реалізації RSA на мові С.

У таблиці 7.11 наведено приклади продуктивності програмної реалізації RSA для 8-бітової експоненти шифрування і різної розрядності модуля.

Таблиця 7.11 – Ефективність програмної реалізації для 8-бітової експоненти шифрування та різної розрядності модуля (в секундах)

Операція	512-бітовий модуль	768-бітовий модуль	1024-бітовий модуль
Шифрування	0,03	0,05	0,08
Розшифрування	0,16	0,48	0,93
Обчислення підпису	0,16	0,52	0,97
Перевірка підпису	0,02	0,07	0,08

Розглянемо проблеми, які виникають під час створення ключів. Ця процедура включає такі завдання:

– визначити два прості числа p та q.
– вибрати e та обчислити d.

Насамперед, варто розглянути проблеми, які пов’язані із вибором p і q. Через те, що значення n=p×q буде відомим потенціальному зловмиснику, для запобігання розкриття p і q ці прості числа повинні необхідно обирати із більшої множини, тобто p і q повинні бути якомога більшими числами. З другого боку, метод, який використовується для пошуку великого простого числа, повинен бути достатньо ефективним.

На сьогодні невідомі ефективні алгоритми, які швидко генерують великі прості числа. Процедура, що використовується для цієї задачі, обирає випадкове непарне число з необхідного діапазону і перевіряє, чи є воно простим. Якщо число не є простим, то обирається інше випадкове число, поки не буде знайдено просте.

Існують різні тести для визначення того, чи є число простим. Ці тести імовірнісні, тобто тест показує, що дане число ймовірно є простим. Незважаючи на це, вони можуть виконуватись таким чином, що дадуть імовірність цього як завгодно близькою до 1. Якщо x не проходить тест, то воно точно складене. Якщо x проходить тест, то воно може бути простим. Якщо x проходить багато таких тестів, то можна з високою імовірністю сказати, що воно просте. Це досить довга процедура, але вона виконується відносно рідко: тільки під час створення нової пари ключів.

На складність обчислень також впливає те, яка кількість чисел буде відкинута перед тим, як буде знайдено просте число. Результат з теорії чисел,

відомий як теорема про просте число, дає зрозуміти, що простих чисел, розташованих близько до x, у середньому, по одному на кожні ln(x) чисел.

Таким чином, у середньому потрібно перевірити послідовність із ln(x) цілих, перш ніж буде знайдено просте число. Через те, що всі парні числа можуть бути відкинуті без перевірки, то потрібно виконати приблизно ln(x)/2 перевірок.

Наприклад, якщо просте число шукають в діапазоні величин 2^{200}, то необхідно виконати близько $\ln(2^{200})/2=70$ перевірок.

Вибравши прості числа p і q, далі слід обрати значення e так, щоб НСД(Φ(n), e)=1 та обчислити значення $d=e^{-1} \bmod \Phi(n)$. Для обчислення d можна використати модифікований алгоритм Евкліда, який дозволяє за фіксований час обчислити найбільший спільний дільник двох чисел, і якщо він дорівнює одиниці, обчислює інверсне значення одного за модулем іншого.

Припустимо тепер, що інформацію, яку перехопив зловмисник, зашифровано на публічному ключі (13, 77). Якою інформацією володіє в такому разі зловмисник? По-перше, він має криптограму «30 01 73 49»; по-друге, має публічний ключ (13, 77). Які зусилля треба йому прикласти для обчислення відкритого тексту? У цьому випадку криптостійкість такого повідомлення наближається до нуля, оскільки розрядність ключа дуже мала. Легко здогадатися, що число 77 єдиним способом розкладається на прості множники, 77=7×11. Можна спостерігати, що компрометація криптосистеми еквівалентна складності розкладання модуля на множники. Це саме, згідно з теоремою Рабіна, справедливо і для великих модулів.

У кінці 1995 р. лише один єдиний раз вдалося практично реалізувати розкриття шифру RSA для 500-бітного ключа. Для цього за допомогою мережі Інтернет було задіяно 1600 комп'ютерів на протязі 5 місяців неперервної роботи. Тому авторами RSA було рекомендовано використовувати таку довжину модуля n:

- 768 біт – для приватних осіб;
- 1024 біти – для комерційної інформації;
- 2048 біт – для особливо таємної інформації.

Постає питання, чи не занадто великі значення модулів? І взагалі, чим повинна визначатися стійкість тієї чи іншої криптосистеми? Для цього спочатку наведемо таблицю типів інформації (табл. 7.12) та час її життя, а також рекомендовану довжину ключа симетричної криптосистеми, яка забезпечує необхідну її стійкість. Доцільно навести також таблицю порівняння криптостійкості симетричних та асиметричних криптосистем (табл. 7.13).

У таблиці вказано, за яких довжин ключів досягається приблизно однакова стійкість симетричних та асиметричних систем до методу суцільного перебору ключів (метод «грубої сили»).

Таблиця 7.12 – Типи інформації та час її життя (в бітах)

Тип інформації	Час життя	Довжина ключа
Тактична військова інформація	хв/год	56-64
Оголошення про нову продукцію, злиття компаній	дні/тижні	64
Довготривалі бізнес-плани	роки	64
Торговельні секрети	10-річчя	122
Секрети водневої бомби	>40 років	128
Особи шпигунів	>50 років	128
Дипломатичні конфлікти	>60 років	128
Дані перепису населення	>100 років	128

Таблиця 7.13 – Порівняння довжин ключів симетричних та асиметричних криптосистем еквівалентної стійкості (в бітах)

Довжина ключа симетричної криптосистеми	Довжина відкритого ключа асиметричної криптосистеми
56	384
64	512
80	768
112	1792
128	2304

Як бачимо, для досягнення однакової стійкості асиметричні криптосистеми прийнято використовувати значно довший ключ (від 7 до 18 разів). Порівнюючи наведені таблиці видно, що з огляду на терміни зберігання інформації різних типів таємності, довжини ключів асиметричних криптосистем у 2048 біт не виглядають занадто параноїдальними.

7.6 Алгоритм Ель-Гамаля

Стійкість криптосистеми Ель-Гамаля, яка була розроблена у 1985 році, ґрунтується на складності задачі дискретного логарифмування у скінченому полі. Для встановлення зашифрованого інформаційного обміну необхідно виконати нижченаведені кроки.

Крок 1. Попередні обчислення. За допомогою криптографічно стійкого генератора випадкових чисел генерують просте число n таке, що обчислення

логарифму за mod n практично важко реалізувати.

Також випадково обирають числа g та a з діапазону [1, n-1] та обчислюють $h=ga\times \bmod n$.

Тепер існує публічний ключ: (n, g, h) та приватний – (n, a).

Крок 2. Шифрування інформації. Зашифровують числа m від 0 до n. Для шифрування виконують таке:

– обирають випадкове число r, яке належить відрізку [1, n-1] та взаємно просте з n-1;

– обчислюють пару чисел C_1 та C_2 за виразами:

$$C_1=g^r\times \bmod n;$$

$$C_2=mh^r\times \bmod n.$$

Пара чисел C_1 та C_2 утворює шифрограму для числа m.

Крок 3. Розшифрування інформації. Розшифрування виконується за формулою:

$$m=C_2(C_1^a)^{-1}\times \bmod n.$$

Доведемо це. Підставимо значення C_1 та C_2 у вираз:

$$m=mh^r(g^a)^{-1}\times \bmod n.$$

Оскільки $h=g^a\times \bmod n$, то:

$$m=mh^r(g^a)^{-1}\times \bmod n=mh^r(h^r)^{-1}\times \bmod n=m.$$

Отже еквівалентність прямого та оберненого перетворення доведена. Криптосистема Ель-Гамаля (з модифікаціями Шнорра) використовується в системах електронного цифрового підпису стандартів в багатьох країнах.

Криптостійкість системи Ель-Гамаля. У реальних застосуваннях, як правило, використовують модуль n криптосистеми довжиною 1024 біти, g – порядку 160 біт.

Безпосередня атака на систему Ель-Гамаля, атака обчислення приватного ключа за публічним, потребує обчислення дискретного логарифму, що для таких великих чисел, n та g перетворюється у математичну задачу надзвичайної обчислювальної складності. Однак імовірна вразливість криптосистеми Ель-Гамаля полягає в тому, що саме повідомлення міститься лише у C_2. Тому теоретично можливою видається атака, коли помноживши C_2 на g^u ($u\neq 0$), отримаємо шифротекст для повідомлення $m^{/}=mg^u$.

Що стосується швидкодії криптосистеми Ель-Гамаля, то швидкість її роботи (на SPARC-M) при програмній реалізації у режимах шифрування та розшифрування зі 160-бітовим показником g для різних довжин модуля n оцінюють величинами, які наведено у таблиці 7.14.

Як видно із наведеної таблиці, швидкість шифрування та розшифрування

значно залежить від довжини модуля: збільшення довжини модуля криптосистеми вдвічі призводить до потрійного зростання часу оброблення.

Таблиця 7.14 – Швидкість роботи криптосистеми Ель-Гамаля на SPARC-M

Режим роботи	Довжина модуля, бітів		
	512	768	1024
Шифрування	0,33 с	0,80 с	1,09 с
Розшифрування	0,24 с	0,58 с	0,77 с

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні операції шифрування в DES.
2. Основні модифікації шифру DES: переваги та недоліки.
3. Структура алгоритмів шифрування.
4. Основні відмінності операцій шифрування в алгоритмах криптографічних перетворень.
5. Блокові та потокові шифри.
6. Основні специфікації операцій шифрування.
7. Режими роботи блоково-симетричних шифрів на основі використання алгоритму DES.
8. Сучасні потокові шифри, їх переваги та недоліки.
9. Модифікації DES та їх режими роботи.
10. Алгоритми криптографічних перетворень.
11. Переваги та недоліки алгоритмів RSA та Ель-Гамаля.

Література: [2; 5-11; 14-17].

Тема 8. Протоколи автентифікації

План:

8.1 Гешувальні алгоритми: призначення та вимоги до них

8.2 Алгоритми сімейства MD

8.3 Алгоритми сімейства SHA

8.1 Гешувальні алгоритми: призначення та вимоги до них

Особливе місце серед механізмів забезпечення цілісності і автентичності займають функції гешування: безключові та ключові, що дозволяють забезпечити широкий спектр послуг безпеки інформації згідно з ISO 7498. Односторонні геш-функції визначаються окремим міжнародним стандартом ISO/IEC 10118.

Вибір та реалізація механізмів забезпечення цілісності та справжності інформаційних ресурсів у сучасних автоматизованих системах є одними з важливих етапів проектування та розробки підсистем захисту інформації. Це пов'язано із постійним зростанням послуг, які надаються різними мережними службами. Більшість послуг надаються при відсутності фіксованих мережених адрес клієнтів та їх особливостей. В зв'язку з цим, ризик порушення цілісності та автентичності інформації збільшується. Для захисту від таких загроз безпеки інформації, як правило, використовують механізми гешування даних – ключові та безключові геш-функції. Геш-функції також можуть використовуватись у складі електронного цифрового підпису, який є потужним механізмом забезпечення автентифікації в сучасних автоматизованих системах.

До обговорення аспектів безпеки варто визначити більш точні визначення геш-функції та її криптографічних властивостей.

Геш-функція – це функція h:D→R, де область визначення D{0,1}* та область значень R{0, 1}^{n} для деякого n≥1.

Компресійна функція – це функція $y_1=h(x_1)$, де D={0,1}^{a}×{0,1}^{b}× і та R={0,1}^{n} для деяких a, b і n≥1 коли a+b≥n.

Ітеративний геш компресійної функції f:({0,1}^{n}×{0,1}^{b}→{0,1}^{n}) – це геш-функція h:({0,1}^{b})→{0,1}^{n}, визначена як:

$$h(X_1, \ldots, X_t)=H_t=H_i=f(H_{i+1}, X_i) \text{ для } 1\le i\le t \text{ (множина } H_0IV).$$

Далі наведені визначення для стійкості за (другим) прообразом і стійкістю до колізій.

Стійкість за прообразом. Геш-функція h:{0,1}→R є стійкою за прообразом ступеня (t, ∈), якщо не існує імовірнісного алгоритму I_h, який приймає вхід Y $\in_R$ R і виводить значення X∈{0,1}* під час виконання не більше t, де h(X)=Y з імовірністю щонайменше ε, отриманою випадковими виборами I_h і Y.

Стійкість за другим прообразом. Нехай S буде кінцевою підмножиною з {0,1}. Геш-функція h:{0,1}*→R є стійкою за другим прообразом ступеня (t, ∈, S), якщо не існує імовірнісного алгоритму S_h, який приймає вхід X $\in_R$ S і виводить значення X′∈{0,1}* під час виконання не більше t, де X′≠Xh(X′)=h(X) ймовірністю щонайменше ε, отриманою випадковими виборами S_h і X.

Геш-функції використовуються як будівельний блок у різних криптографічних додатках. Найбільш важливе їх використання для захисту автентифікації інформації і як інструмент для схем цифрових підписів. Геш-функція – це функція, яка відображає вхід довільної довжини в фіксоване число вихідних біт – геш-значення. Для того щоб бути корисною в криптографічних додатках, геш-функція повинна задовольняти деякі вимоги. Геш-функції можуть

поділятися на односторонні гешфункції та стійкі до колізій геш-функції.

Одностороння функція повинна бути стійкою за прообразом і другим прообразом, тобто повинно бути «важко» знайти повідомлення із заданим гешем (прообразом) або яке гешується в одне і те ж значення, що і задане повідомлення (другий прообраз).

Стійка до колізій геш-функція – це одностороння геш-функція, для якої «важко» знайти два різні повідомлення, для яких геш-значення однакове.

Для деяких програм можуть знадобитися додаткові властивості до геш-функцій, наприклад, псевдовипадковість виходу, що генерується. У контраст до інших криптографічних примітивів, обчислення геш-функції не залежить від будь-якої секретної інформації.

Одностороння геш-функція – це функція h, яка задовольняє такі умови: аргумент X може бути довільної довжини, а результат h(X) має фіксовану довжину n біт; геш-функція повинна бути односторонньою в тому сенсі, що за заданим Y в образі h складно знайти повідомлення X таке, що h(X)=Y (стійкі за прообразом) і за заданим повідомленням X і значенням h(X) важко знайти повідомлення $X' \neq X$ таке, що $h(X')=h(X)$ (стійкі за другим прообразом).

Стійка до колізій геш-функція – це функція h, яка задовольняє такі умови:

– аргумент X може бути довільної довжини, а результат h(X) має фіксовану довжину n біт;

– геш-функція повинна бути односторонньою, тобто стійкою за прообразом і стійкою за другим прообразом.

Для того, щоб геш-функція H вважалася криптографічно стійкою, вона повинна задовольняти три основні вимоги, на яких заснована більшість застосувань геш-функцій в криптографії:

– незворотність або стійкість до відновлення прообразу: для заданого значення геш-функції m має бути обчислювально неможливо знайти блок даних x, для якого m h(x)=m;

– стійкість до колізій першого роду або відновлення другий прообразів: для заданого повідомлення m повинно бути обчислювально неможливо підібрати інше повідомлення n, для якого h(n)=h(m);

– стійкість до колізій другого роду: має бути обчислювально неможливо підібрати пару повідомлень, що мають однаковий геш.

Ці вимоги не є незалежними:

– оборотна функція нестійка до колізій першого і другого роду;

– функція, нестійка до колізій першого роду, нестійка до колізій другого роду;

– зворотне неправильне.

Односторонні геш-функції можуть застосовуватися для вирішення інших завдань, наприклад, вироблення ключів і псевдовипадкових чисел. Для застосування в таких завданнях геш-функція повинна задовольняти такі вимоги:

– відсутність кореляції – вхідні і вихідні біти не повинні корелювати, тобто зміна будь-якого вхідного біта призводить до великих непередбачуваним змін вихідних бітів;

– стійкість до близьких колізій – для заданої односторонньої функції обчислювально неможливо знайти два прообрази X і $X^{/}$, для яких геш-значення h(X) і h($X^{/}$) відрізнялися б на малу кількість біт;

– стійкість до часткової односторонності – обчислювально неможливо відновити будь-яку частину вхідного повідомлення так само, як і всі повідомлення, більш того, за будь-якої відомої частини вхідного повідомлення обчислювально неможливо відновити частину (відновлення t невідомих біт вимагає не менш за 2^{t-1} операцій);

– можливість роботи в режимі розтягування – можливість обчислення геш-функції при довжині вхідного повідомлення менше ніж довжина геш-значення.

Вимога до застосовуваних у криптографії геш-функцій з секретним ключем: обчислювальна стійкість – неможливість знаходження геш-значення для заданого повідомлення без відомого секретного ключа, тобто для заданої ключовою геш-функції і однієї або більше коректних пар прообразів і геш-значень (x_i, h(x_i, k)) та невідомому секретному ключі k обчислювально неможливо знайти іншу коректну пару (x, h(x, k)) для будького і $x \neq x_i$.

Вимога обчислювальної стійкості передбачає виконання вимоги стійкості ключа (за однією або більше коректних пар прообразів і геш-значення (x_i, h(x_i, k)) обчислювально неможливо відновити секретний ключ), однак вимога стійкості ключа k не передбачає виконання вимоги обчислювальної стійкості.

Більшість геш-функцій мають ітеративні конструкції в тому сенсі, що вони базуються на функції компресії з фіксованими входами, вони обробляють кожен блок повідомлення подібним чином. Введення X доповнюється за однозначним правилом доповнення до кратності розміру блоку. Зазвичай це також включає додавання загальної довжини входу в бітах. Доповнений вхід потім ділиться на t блоків, які охоплюють від X_1 до X_t. Геш-функція включає компресійну функцію f і зв'язує змінну H_i між стадією i-1 та стадією i.

Класифікацію геш-функцій наведено на рисунку 8.1.

До безключових геш-функцій відносяться коди виявлення змін

повідомлення (MDC-код, modification detection code), також відомі як коди виявлення маніпуляцій над повідомленнями або коди цілісності повідомлень.

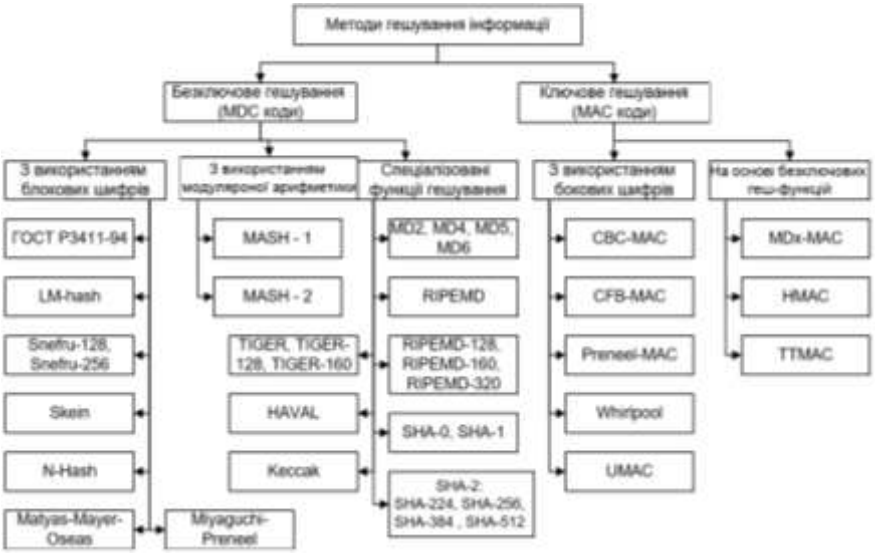

Рисунок 8.1 – Класифікація геш-функцій

Суттєвим недоліком безключових геш-функцій є те, що вони не захищені від можливості по підбору такого ж самого повідомлення з однаковим гешем, та мають відсутність властивості обчислювальної стійкості. Зрештою MDC-коди забезпечують, спільно з іншими механізмами, цілісність даних.

До ключових геш-функцій відносяться MAC-коди.

Визначення автентифікуючих кодів повідомлення за Пренилем (Preneel): MAC-функція h, повинна задовольняти нижче перераховані умови.

1. Аргумент X може бути довільної довжини й результат h(K, X) має фіксовану довжину n біт, де вторинний вхід K позначає секретний ключ.

2. При наявності даних h і X (але з невідомим K) складно визначити h(K, X) з імовірністю успіху значно більшою за $1/2^n$.

За умови коли відомо про велику кількість пар $\{X_i, h(K, X_i)\}$ складно визначити ключ K або обчислити $h(K, X')$ для будь-якого $X' \neq X_i$.

Більшість MAC є повторюваними конструкціями, у тому розумінні, що вони засновані на функції стискання із фіксованим розміром вхідних значень; вони обробляють кожний блок повідомлень аналогічниим способом. Вхід X є однозначним заповненням, кратним розміру блоку. Звичайно це також включає

збільшення загальної довжини на бітах вхідних значень. Заповнений вхід потім розділяється на t блоків, що позначають X_1 через X_t. MAC включає функцію стискання f і єднальну змінну H_i між етапом i-1 та етапом i:

$$H_0=IV_K;\ H_i=f_K(H_{i-1}, X_i),\ 1\le i\le t;$$

$$h(K, X)=g_K(H_t).$$

Тут IV вказує на початкове значення, а g – вихідне перетворення. Секретний ключ K може бути застосований в IV, у функції стискання, і/або у вихідному перетворенні.

Існує декілька алгоритмів, які розроблено для специфічної мети автентифікації повідомлення. У більшості випадків код автентифиікації повідомлення створюється із блокового шифру або з геш-функції. Різні методи є сімействами універсальних геш-функцій. Також поєднують процедури, початі декількома організаціями для стандартизації кодів автентифікації повідомлення.

MAC на основі блокового шифру. Найбільш загальним шляхом використання MAC у блоковому шифрі є використання шифру в режимі CBC (блокове з'єднання шифру): ключ MAC використовується як код на кожному кроці ітерації, і блок повідомлення, що обробляється на поточній ітерації, виступає у якості перекладу відкритого тексту в шифр, після побітового додавання з вихідним значенням шифротекста з попереднього кроку:

$$H_1=E_k(X_1),\ H_i=E_K(X_i \oplus H_{i-1}),\ 2\le i\le t.$$

Тут припускається, що повідомлення X (після заповнення), ділиться на $X_1, .., X_t$ блоків з довжиною, що відповідає блокового шифру, який використовується. E_K означає шифрування із секретним ключем K, а H_t формує вихідне значення алгоритму MAC.

Окремо можна виділити три підходи побудови MAC-кодів.

1. MAC-коди, які побудовано на основі БСШ (CBC-MAC).

2. MAC-коди, які побудовано на основі безключових геш-функцій (HMAC, MDX-MAC).

3. MAC-коди, які побудовано на основі сімейства універсальних геш-функцій.

Основна конструкція CBC підходить для атаки exor-підробки, отже, може бути використана в додатках, де повідомлення мають фіксовану довжину. Трохи більш безпечні зміни в схемі, проте, існують.

Прикладом є алгоритм EMAC – це використання додаткового шифрування як вихідного перетворення, де ключ шифрувальної операції може бути похідний від ключа MAC. Інший приклад, відомий як перерозподіл MAC, заміняє останнє шифрування двоключовим потрійним шифруванням. Безпека цих конструкцій

може бути доведена на основі припущення, що основний блоковий шифр – псевдовипадковий.

Усі ці схеми включені в ISO/IEC 9797-1, стандарт для MAC, що використовує (невизначений) блоковий шифр.

Розробку нових методів виробітку CBC-MAC обумовило появу нових атак на CBC-MAC, що докладно описуються в додатку A ISO/IEC 9797-1. В оновлений стандарт увійшли новий метод доповнення повідомлення і новий алгоритм формування MAC-коду зі спеціальною обробкою першого блоку (такий же, як і обробка останнього блоку). Це робить більш трудомістким вичерпний пошук ключа. Крім того, стандартом вводяться два нових «рівнобіжних» варіанти формування CBC-MAC.

Сутність нового методу доповнення полягає у наступному. Рядок даних x доповнюється праворуч необхідною кількістю нулів (можливе доповнення і не нулів) до одержання рядка, довжина якого буде кратною n бітам. Потім отриманий рядок доповнюється ліворуч одним n-розрядним блоком L, що містить двійкове представлення довжини, вираженої в бітах, нерозширеної рядка даних x. При необхідності додатковий блок заповнюється ліворуч нулями до довжини n. У новій версії ISO/IEC 9797-1 пропонується шість алгоритмів виробітку MAC-кодів. Перші три алгоритми описані стандартом за 1994 рік.

Алгоритм 1. Перший алгоритм є просто виробітком CBC-MAC без якої-небудь додаткової обробки.

Алгоритм 2 є виробітком CBC-MAC з додатковою обробкою другого типу (з додатковим шифруванням останнього блоку на ключі k').

Алгоритм 3 є виробітком CBC-MAC з додатковою обробкою першого типу (з додатковим дешифруванням на ключі k' і шифруванням останнього блоку на ключі k). Таким чином, останній блок піддається потрійному шифруванню.

Алгоритм 4. У цьому алгоритмі перший і останній блоки повідомлення піддаються подвійному шифруванню.

Алгоритм 5. Алгоритм будується на принципі рівнобіжного застосування двох алгоритмів 1 з різними ключами. Два вихідних значення потім складаються за модулем 2, утворити результуючий MAC-код.

Алгоритм 6. Алгоритм також будується на принципі рівнобіжного застосування двох алгоритмів з різними ключами. Тільки як основа береться алгоритм 4. Два вихідних значення складаються за модулем 2, утворити результуючий MAC-код.

MAC на основі геш-функцій. Код автенфікації повідомлення може бути також отриманий з геш-функції, включаючи секретний ключ в обчисленні. Це

найбільш загальний метод, оскільки такі MAC звичайно швидше, ніж MAC на основі блокового шифру. Проте просто додаючи або додаючи ключовий фрагмент на вхід повідомлення геш-функції не дає безпечний MAC.

HMAC – вкладена конструкція, яка обчислює MAC для основної функції геша h, повідомлення X і секретний ключ K таким способом:

$$HMAC(K, X)=h(K \oplus opad)||h((K \oplus ipad)||X))).$$

Ключ K спочатку заповнюється нульовими бітами (opad та ipad – сталі величини). Беллейр (Bellare) довів безпеку цієї конструкції такими припущеннями:

– основна функція геша є стійкої до помилок для секретної початкової величини;

– функціональної за ключем стискання початкової величини – безпечний алгоритм MAC (для повідомлень одного блоку);

– функція стискання є слабкою псевдодовільною функцією.

Альтернативою для HMAC є конструкції MDx-MAC, які можуть бути засновані на MD5, SHA, RIPEMD або аналогічних функціях геша.

Тут, основна геш-функція перетворена в MAC невеликими модифікаціями, включаючи секретний ключ на початку, в остаточному підсумку й у кожній ітерації функції геша. Це досягається ключовими залежними модифікаціями початкової величини й константи значення, що додається, яке використовується геш-функцією, і вихідним перетворенням, залежним від ключа. Безпека MDx-MAC може бути доведена на основі припущення, що основна функція стискання псевдодовільна.

Як HMAC, так і MDx-MAC включені в ISO/IEC 9797-2, стандарт для MAC, що використовував власну геш-функцию.

MAC, які засновані на універсальному гешуванні. Сімейство геш-функцій геша $H=\{h:D\rightarrow R\}$ – це кінцева множина функцій із загальною областю визначення D і (кінцевим) діапазоном R. Його можна також позначити через $H:K\times D\rightarrow R$, де $H_k:D\rightarrow R$ – функція множини для кожного $K\in K$. В останньому випадку можна вибрати довільну функцію h з множини $K\in K$ та $h=HK$.

Множина універсальних геш-функцій є сімейством геш-функцій з деякою комбінаторною властивістю. Наприклад, сімейство геш-функцій $H=\{h:D\rightarrow R\}$ є майже універсальним, якщо для будь-якого різного X, $X'\in D$, імовірність, що $h(X)= h(X')$ – не більш, ніж коли $h\in H$ вибирається довільно.

Це може використовуватися для автентифікації повідомлення, наприклад при гешуванні повідомлення з функцією із сімейства універсальних геш-функцій, що кодує вихід геша, й потім здійснює закодований вихід геша як

величину MAC. Це підтверджується тим, що безпека результуючої схеми MAC залежить від безпеки шифру, використаного для кодування вихідного геша. Комбінаторні властивості сімейства універсальних геш-функцій часто нескладно довести і схеми, що отримуються на виході є найшвидшими серед MAC. Різновид NESSIE UMAC – приклад MAC, заснований на універсальній геш.

Сучасні стандарти. Декілька організацій здійснюють ініціативи стандартизації автентифікації кодів повідомлення. ISO/IEC розробив стандарт 9797 для MAC у двох окремих частинах. Частина 9797-1 описує MAC, заснований на блоковому шифрі, а саме CBC-MAC для невизначеного блокового шифру (з деякими додатковими розширеннями, включаючи EMAC і перерозподіл-MAC). Розділ 9797-2 деталі MAC засновані у відданій функції геша, а саме HMAC і конструкції Mdx-mac для невизначеної геш-функції (варіант Mdx-mac для коротких вхідних значень).

ANSI прийняв базований DES CBC-MAC (включаючи перерозподіл MAC) у своєму стандарті X9.19 і HMAC (з невизначеною гешфункцією) у стандарті X9.71. NIST розробив FIPS 113 для DES CBCMAC і FIPS 198 для SHA-1 HMAC.

Рівень безпеки залежить від розміру внутрішнього блоку (розмір блоку функції гешування), від довжини ключа і від довжини значення MAC-коду. Серед основних недоліків алгоритмів, які вже розглянуті, є погане розсіювання та використання для генерації ключа алгоритму DES (AES). Щодо використання алгоритмів DES та AES для отримання стійкої ключової послідовності, то це накладає обмеження на швидкість гешування самого алгоритму MAC-коду. У таблиці 8.1 наведено аналіз тестування швидкості роботи алгоритмів гешування.

У таблиці 8.2 наведено можливі значення довжин ключа і геш-коду для різних алгоритмів сімейства MAC.

У таблиці 8.3 наведено основні результати оцінки швидкодії MAC-алгоритмів для різних операційних платформ. Швидкість обчислень визначається кількістю циклів процесора, які затрачуються на один байт оброблюваного повідомлення. Аналіз таблиці 8.3 дозволяє зробити висновок, що схеми ключового гешування UMAC на основі поліноміальних функцій дозволяють одержати найвищу швидкість гешування.

Геш-функції RIPEMD-160, RIPEMD-128. У 1995 році були виявлені деякі недоліки в першій версії гешфункції RIPEMD, що формує 128-розрядний геш-код. Зокрема, були виявлені колізії для останніх двох із трьох циклів RIPEMD. Розроблена методика пошуку колізій була успішно застосована і для пошуку колізій у MD4. На основі отриманих результатів були зроблені припущення, що ця методика може бути використана для пошуку колізій у MD5 і в повній версії

RIPEMD. Версія RIPEMD (разом з SHA-1) широко використовується в банківських технологіях. Однак ситуація з криптоаналізом гешфункцій сімейства MDx і перспективи розвитку обчислювальних потужностей призвели до висновку про необхідність відновлення RIPEMD. У результаті для стандартизації були запропоновані більш кращі версії геш-функції – RIPEMD-160 і RIPEMD-128. За оцінками розроблювачів геш-функція RIPEMD-160 повинна залишатися безпечною протягом десяти найближчих років. Удосконалена версія RIPEMD-128 замінила геш-функцію RIPEMD.

Таблиця 8.1 – Аналіз тестування швидкості роботи алгоритмів гешування

Функція гешування	Кількість циклів	Мова реалізації	Швидкість роботи на Celeron 600 MHz	Швидкість роботи на Pentium III 1000 MHz
Whirlpool	10	C	28,013 Мбіт/с	46,961 Мбіт/с
SHA-2 (512)	80	C	41,159 Мбіт/с	68,701 Мбіт/с
SHA-2 (256)	64	C	81,308 Мбіт/с	135,557 Мбіт/с
ГОСТ 34311-95	–	C+Assembler	49,408 Мбіт/с	83,056 Мбіт/с
HAVAL	96(128, 160)	C	337,842 Мбіт/с	564,809 Мбіт/с
SHA-1	80	C, Assembler	206,285 Мбіт/с 361,581 Мбіт/с	344,433 Мбіт/с 605,558 Мбіт/с
RIPEMD-160	160	C	147,465 Мбіт/с	246,568 Мбіт/с
MD5	64	C	278,715 Мбіт/с	574,635 Мбіт/с
MD4	48	C	344,086 Мбіт/с	467,793 Мбіт/с
UMAC	–	C, C+Assembler	989,371 Мбіт/с 3518,900 Мбіт/с	1648,953 Мбіт/с 5885,057 Мбіт/с
Rijndael CBC-MAC	14	C	139,376 Мбіт/с	231,255 Мбіт/с
ГОСТ 28147-89	16	C+Assembler	189,559 Мбіт/с	315,270 Мбіт/с

Таблиця 8.2 – Довжина ключа k і довжина геш-коду n для MAC-кодів

Алгоритм	k (ключ)	n (геш-код)
UMAC	128	64
TTMAC	160	≤160
EMAC-AES	128, 192, 256	≤128
RMAC-AES	128, 192, 256	≤128
HMAC-SHA-1	≤512	≤160

Таблиця 8.3 – Швидкодія MAC-алгоритмів

Алгоритм	Довжина MAC-коду (біти)	Довжина ключа (біти)	Тип ПК				
			Pentium2	PIII/Linux	Pentium4	Xeon	AMD
TTMAC	160	160	21	21	40	37	21
UMAC-16	64	128	6,1	6,0	6,2	6,1	6,2
UMAC-32	64	128	2,5	2,9	6,7	6,6	1,9
HMACWhirlpool	512	512	86	72	98	103	100
HMAC-MD4	128	512	4,7	4,7	6,4	6,4	4,7
HMAC-MD5	128	512	7,2	7,3	9,4	9,4	7,4
HMACRIPE-MD	160	512	23	18	27	26	21
HMAC-SHA-0	160	512	16	15	23	23	13
HMAC-SHA-1	160	512	16	15	25	24	12
HMAC-SHA2	256 384 512	512	40 84 84	39 84 84	40 124 124	39 132 132	33 72 72
HMAC-Tiger	192	512	24	21	28	26	20
CBC MAC-Rijndael (EMAC)	128	128	24	26	26	27	31
CBC MACDES	64	56	62	61	72	69	54
CBC MAC-Shacal	512	160	31	31	67	74	29

Розглянемо ці функції більш детально. Розмір геш-кода і перемінних зчеплень RIPEMD-160 дорівнює 160 бітам (п’ять 32-х розрядних слів). Кількість циклів збільшена з трьох (як у RIPEMD) до п’яти. Крім того, внесені додаткові зміни в паралельні лінії алгоритму. Тепер права і ліва лінії відрізняються не

тільки застосовуваними константами, але і порядком проходження бульових функцій. Для алгоритму RIPEMD-160 визначені такі бульові функції:

$$f(u,\ v,\ w) = u \oplus v \oplus w;\ g(u,\ v,\ w) = (u \wedge v) \vee (\overline{u} \wedge w);$$

$$h(u,\ v,\ w) = (u \wedge \overline{v}) \oplus w;\ k(u,\ v,\ w) = (u \wedge w) \vee (v \wedge \overline{w});$$

$$l(u,\ v,\ w) = u \oplus (v \wedge \overline{w}).$$

Усі позначення аналогічні до тих, які були раніше використані під час опису алгоритму SHA-1. На рисунку 8.2 подано загальну структуру геш-функції RIPEMD-160.

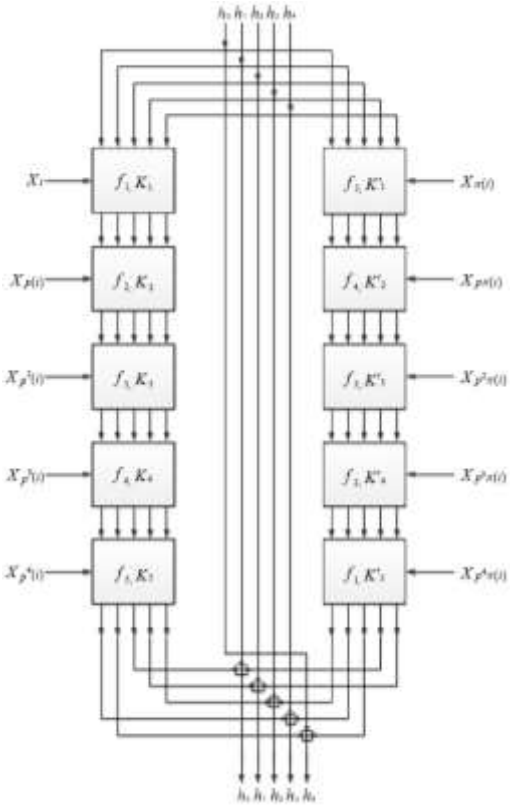

Рисунок 8.2 – Схема геш-функції RIPEMD-160

Деякі додатки, у яких використовують геш-функції, можуть вимагати виробітки більш довгих геш-кодів. Прямим шляхом розв'язання цієї задачі є паралельне виконання однієї і тієї ж геш-функції з різними векторами

ініціалізації. Однак у цьому випадку можлива поява залежностей між двома результатами гешування, що і було виявлено при використанні MD4. Геш-функції RIPEMD-128 і RIPEMD-160 уже мають паралельні лінії і для одержання геш-кодів довжиною, відповідно, 256 і 320 біт досить виключити кінцеву комбінацію результатів гешування по кожній лінії.

8.2 Алгоритми сімейства MD

Спеціалізовані геш-функції (Customised hash functions або dedicated hash functions) розроблені спеціально для цілей гешування й оптимізовані для виконання цієї задачі. Третя частина стандарту ISO/IEC 10118-3 визначає три спеціалізовані геш-функції, а саме функції RIPEMD-128, RIPEMD-160 і SHA-1. Ці геш-функції засновані на використанні принципів побудови, закладених у геш-функції сімейства MDx (MD2, MD4, MD5), які спеціально розроблялися для реалізації на 32-розрядних ЕОМ.

Алгоритм MD4 був запропонований Рональдом Райвестом у 1990 році, а в 1991 авторм було запропоновано модифіковану версію алгоритму – MD5. У даний час геш-функції MD4, MD5 є найбільш розповсюдженими в практичних додатках геш-функціями, однак Р. Райвест у 2010 році визнав її небезпечною і запропонував не використовувати під час розроблені програмних продуків. Окрім цього деякі їх недоліки не дозволили стандартизувати їх на міжнародному рівні.

Європейський консорціум RIPE, спираючись на свої дослідження властивостей цих алгоритмів, запропонував посилену версію MD4, що одержала назву RIPEMD. Геш-функція RIPEMD по суті складається з двох паралельно працюючих і модифікованих функцій MD4, тобто функція має дві лінії. Іншою альтернативою алгоритмам MDx є алгоритм SHA-1, розроблений спільно Агентством національної безпеки США і NIST і прийнятий як американський національний стандарт (FIPS 180-1).

MD4. MD4 (Message Digest 4) – геш-функція, розроблена Рональдом Рівестом професором Массачусетського університету в 1990 році, а вперше описана в RFC 1186. Для довільного вхідного повідомлення функція генерує 128-розрядне геш-значення, яке називається дайджестом повідомлення. Цей алгоритм використовується в протоколі автентифікації MSCHAP, розробленому корпорацією Майкрософт для виконання процедур перевірки достовірності віддалених робочих станцій Windows.

Гешування з MD4 складається з 48 операцій, згрупованих в 3 раунди по 16 операцій. F-нелінійна функція і в кожному раунді вона змінюється. M_i відповідає

за 32-бітний блок вхідного повідомлення, а K_i – 32-бітова константа, яка відрізняється для кожної операції.

На рисунку 8.3 наведено структуру раунда MD4.

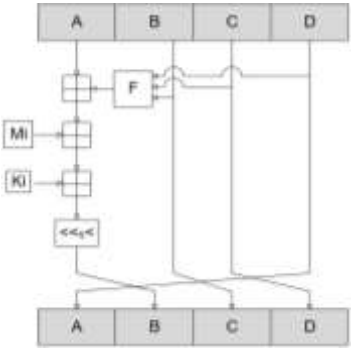

Рисунок 8.3 – Структура раунда MD4

Алгоритм MD4. Передбачається, що на вхід подано повідомлення, яке складається із біт, геш якого необхідно обчислити. Тут – довільне невід'ємне ціле число, воно може бути нулем, не повинно бути кратним восьми, і може бути як завгодно великим.

Запишемо повідомлення побітово, а саме: $m=m_0m_1…m_{b-1}$.

Далі подано 5 кроків, які прийнято використовувати для обчислення гешу повідомлення.

Крок 1. Додавання відсутніх бітів. Повідомлення розширюється так, щоб його довжина в бітах за модулем 512 дорівнювала 448. Таким чином, у результаті розширення, повідомленням бракує 64 біти до довжини, кратної 512 бітам. Розширення проводиться завжди, навіть якщо повідомлення спочатку має необхідну довжину.

Розширення проводиться таким чином: один біт, що дорівнює 1, додається до повідомлення, а потім додаються біти, рівні 0, до тих пір, поки довжина повідомлення не стане рівною 448 за модулем 512.

У результаті до повідомлення додається як мінімум 1 біт, і як максимум 512.

Крок 2. Додавання довжини повідомлення. 64-бітове уявлення b (довжини повідомлення перед додаванням набивальних бітів) додається до результату попереднього кроку. У малоймовірному випадку, коли b більше, ніж 2^{64} використовуються тільки 64 молодших біти. Ці біти додаються у вигляді двох 32-бітових слів, і першим додається слово, що містить молодші розряди.

На цьому етапі (після додавання бітів і довжини повідомлення) отримуємо повідомлення довжиною, кратною 512 бітам. Це еквівалентно тому, що це повідомлення має довжину, кратну 16-ти 32-бітовим словами. Кожне 32-бітове слово містить чотири 8-бітних, але йдуть вони не підряд, а навпаки (наприклад, з восьми 8-бітових слів (abcdefgh) отримуємо два 32-бітових слова (dcba hgfe)).

Нехай M[0…N-1] означає масив слів отриманого повідомлення (де N кратне 16).

Крок 3. Ініціалізація MD-буфера. Для обчислення гешу повідомлення використовується буфер, який складається із 4 слів (32-бітних регістрів): (A, B, C, D). Ці регістри ініціалізувалися такими шістнадцятковим числами (молодші байти спочатку):

word A: 67 45 23 01;
word B: ef cd ab 89;
word C: 98 ba dc fe;
word D: 10 32 54 76.

Крок 4. Обробка повідомлення блоками по 16 слів. Для початку необхідно визначити три допоміжні функції, кожна з яких отримує на вхід три 32-бітових слова, і за ними обчислює одне 32-бітове слово.

$$F(X,\ Y,\ Z) = XY;\quad F(X,\ Y,\ Z) = XY \vee XZ;$$

$$G(X,\ Y,\ Z) = XY \vee XZ \vee YZ;\quad H(X,\ Y,\ Z) = XYZ.$$

На кожну бітову позицію F впливає умовний вираз: якщо не X, то Y, а інакше Z. Функцію F можна було б визначена із використання $\oplus$ замість V, оскільки XY і XZ не можуть бути рівними «1» одночасно. G впливає на кожну бітову позицію як функція максимального значення: якщо, щонайменше, в двох словах з X, Y, Z відповідні біти рівні 1, то G видасть 1 в цьому біті, а інакше G видасть біт, що дорівнює 0. Зазначимо, що якщо біти X, Y і Z статистично незалежні, то біти F(X, Y, Z) і G(X, Y, Z) будуть також статистично незалежні. Функція H реалізує побітовий XOR, вона володіє такою ж властивістю, як і F або G.

Крок 5. Формування гешу. Результат (геш-функція) виходить як ABCD. Тобто треба виписати 128 біт, починаючи з молодшого біта A, а закінчуючи старшим бітом D.

Реалізація алгоритму мовою C міститься в RFC 1320.

Порівняння MD4 з MD5. MD4 використовує три цикли з 16 кроків кожен, в той час, як MD5 використовує чотири цикли з 16 кроків кожен.

У MD4 додаткова константа в першому циклі не застосовується. Аналогічна додаткова константа використовується для кожного із кроків у

другому циклі. Інша додаткова константа використовується для кожного з кроків в третьому циклі. У MD5 різні додаткові константи T[i] застосовуються для кожного із 64 кроків.

MD5 використовує чотири елементарні логічні функції, по одній на кожному циклі, порівняно з трьома в MD4, по одній на кожному циклі.

У MD5 на кожному кроці поточний результат складається з результатом попереднього кроку. Наприклад, результатом першого кроку є зміненим словом A. Результат другого кроку зберігається в D і утворюється додаванням A до циклічно зрушеному вліво на певне число біт результату елементарної функції. Аналогічно, результат третього кроку зберігається в C і утворюється додаванням D до циклічно зрушеному вліво результату елементарної функції. MD4 це останнє додавання не включає.

Безпека. Рівень безпеки, який закладався в MD4, був розрахований на створення досить стійких гібридних систем електронного цифрового підпису, заснованих на MD4 і криптосистеми з відкритим ключем. Рональд Рівест вважав, що алгоритм гешування MD4 можна використовувати і для систем, які потребують сильної криптостійкості. Але в той же час він зазначав, що MD4 створювався передусім як дуже швидкий алгоритм гешування, тому він може бути поганим в плані криптостійкості.

Як показали дослідження, він був правим, і для додатків, де важлива насамперед крипостійкість, став використовуватися алгоритм MD5.

Вразливості. Вразливості в MD4 були продемонстровані у статті Берта ден Боєра і Антона Босселаріса в 1991 році. Перша колізія була знайдена Гансом Доббертіном в 1996 році.

MD2. MD2 (The MD2 Message Digest Algorithm) – геш-функція, розроблена Рональдом Рівестом (RSA Laboratories) в 1989 році, і описана в RFC 1319.

Розмір геша – 128 біт. Розмір блоку вхідних даних – 512 біт.

Алгоритм MD2. Передбачається, що на вхід подано повідомлення, що складається із b байт, геш якого нам належить обчислити (тут b – довільне невід'ємне ціле число, воно може бути нулем або будь-яким завгодно великим). Запишемо повідомлення побайтово, у вигляді: $m=m_0m_1\ldots m_{b-1}$.

Обчислення гешу повідомлення відбувається за наступними кроками:

Крок 1. Додавання відсутніх біт. Повідомлення розширюється так, щоб його довжина в байтах за модулем 16 дорівнювала 0. Таким чином, у результаті розширення довжина повідомлення стає кратною 16 байтам. Розширення проводиться завжди, навіть якщо повідомлення спочатку має потрібну довжину.

Розширення зазвичай проводиться наступним чином: і байт, які рівні і,

додаються до повідомлення, так щоб його довжина в байтах стала рівною 0 за модулем 16. Після чого до повідомлення додають як мінімум 1 байт (максимум 16).

На цьому етапі (після додавання байт) повідомлення має довжину в точності кратну 16 байтам. Нехай M[0…N-1] означає байти отриманого повідомлення (N кратні 16).

Крок 2. Додавання контрольної суми. 16-байтна контрольна сума повідомлення додається до результату попереднього кроку. Цей крок використовує 256-байтову «випадкову» перестановчу матрицю, яка складається із цифр числа пі (PI_SUBST [256]).

Крок 3. Формування гешу. Геш обчислюють як результат X[0…15], на початку йде байт X[0], а в кінці X[15].

На цьому опис алгоритму MD2 завершується.

В RFC 1319 можна знайти реалізацію алгоритму мовою С.

Безпека. Роже і Шаво в 1997 році опублікували приклад колізій для MD2, хоча і не змогли представити алгоритм знаходження інших колізій. У 2004 році було показано, що MD2 схильний до атак на знаходження колізій зі складністю, яка еквівалентна 2104 операцій гешування. У 2004 Міллер заявив, що MD2 не може більше розглядатися, як криптостійкий алгоритм гешування.

MD5. MD5 – це поліпшена версія MD4. Хоча вона складніша за MD4, їх схеми схожі, і результатом MD5 також є 128-бітове значення. На рисунку 8.4 наведено структуру раунда MD5.

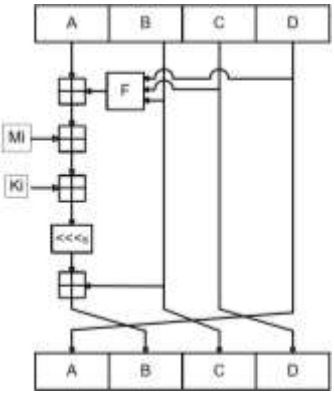

Рисунок 8.4 – Структура раунда MD5

Розглянемо алгоритм отримання дайджеста повідомлення MD5 (RFC 1321), розроблений Р. Рівестом.

Логіка виконання MD5. Алгоритм отримує на вході повідомлення довільної довжини і створює в якості виходу дайджест повідомлення довжиною 128 біт. Логіку виконання наведено на рисунку 8.5.

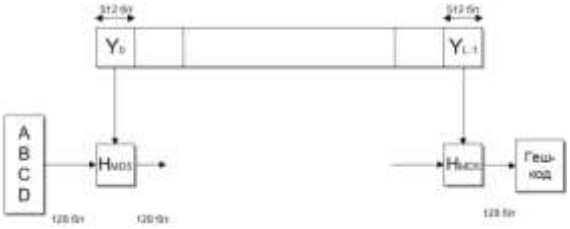

Рисунок 8.5 – Логіка виконання MD5

Алгоритм складається із нижче наведених кроків.

Крок 1. Додавання відсутніх бітів. Повідомлення доповнюється таким чином, щоб його довжина стала дорівнювати 448 за модулем 512 (довжина 448 mod 512). Це означає, що довжина доданого повідомлення на 64 біта менша, у порівнянні із числом, кратним 512. Додавання виробляється завжди, навіть, у тих випадках, коли повідомлення має необхідну довжину. Наприклад, якщо довжина повідомлення 448 бітів, воно доповнюється 512 бітами до 960 бітів. Таким чином, число біт, що додаються, знаходиться в діапазоні від 1 до 512.

Додавання складається з одиниці, за якою слідує необхідна кількість нулів.

Крок 2. Додавання довжини. 64-бітове уявлення довжини вихідного (до додавання) повідомлення в бітах приєднується до результату першого кроку. Якщо першопочаткова довжина більша за 2^{64}, то використовують тільки останні 64 біти. Таким чином, поле містить довжину вихідного повідомлення за модулем 2^{64}.

У результаті перших двох кроків створюється повідомлення, довжина якого кратна 512 бітам. Це розширене повідомлення, яке подано на рисунку 8.6, подається як послідовність 512-бітних блоків Y_0, Y_1, …, Y_{L-1}, при цьому загальна довжина розширеного повідомлення дорівнює L×512 бітам. Таким чином, довжина отриманого розширеного повідомлення кратна шістнадцяти 32-бітовим словами.

Крок 3. Ініціалізація MD-буфера. Зазвичай використовують 128-бітний буфер для зберігання проміжних і остаточних результатів геш-функції. Буфер може бути представлений як чотири 32-бітних регістри (A, B, C, D). Ці регістри ініціалізувалися такими шістнадцятковим числами:

A=01234567; B=89ABCDEF; C=FEDCBA98; D=76543210.

Рисунок 8.6 – Структура розширеного повідомлення

Крок 4. Оброблення послідовності 512-бітних (16-слівних) блоків

Основою алгоритму є модуль, який складається із чотирьох циклічних обробок, та позначений HMD5. Чотири цикли мають схожу структуру, але кожен цикл використовує свою елементарну логічну функцію, що позначається f_F, f_G, f_H та f_I відповідно. На рисунку 8.7 наведено послідовність обробки 512-бітного блоку.

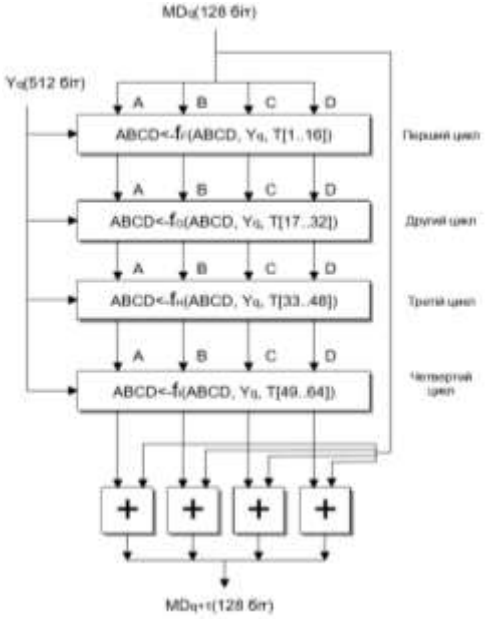

Рисунок 8.7 – Обробка чергового 512-бітного блоку

Кожен цикл приймає на вході поточний 512-бітний блок Y_q, який обробляється в даний момент, і 128-бітове значення буферу ABCD, яке є проміжним значенням дайджесту, і змінює вміст цього буфера. Кожен цикл також використовує четверту частину 64-елементної таблиці T[1…64], побудованої на основі функції sin. і-ий елемент T, який прийнято позначати через T[i], має значення, яке дорівнює цілій частині від 2^{32}×abs(sin(i)), яка задана в радіанах.

Оскільки abs(sin(i)) є числом між 0 і 1, то кожен елемент T є цілим, яке може бути представлено 32 бітами. Таблиця забезпечує «випадковий» набір 32-бітних значень, які повинні ліквідувати будь-яку регулярність у вхідних даних. Для отримання MD_{q+1} вихід чотирьох циклів додається за модулем 2^{32} з MD_q. Додавання відбувається незалежно для кожного з чотирьох слів у буфері.

Крок 5. Вихід. Після обробки всіх L 512-бітних блоків виходом L-ої стадії є 128-бітний дайджест повідомлення

Розглянемо більш детально логіку кожного із чотирьох циклів виконання одного 512-бітного блоку. Кожен цикл складається з 16 кроків, що оперують із буфером ABCD. Логіку виконання окремого кроку наведено на рисунку 8.8.

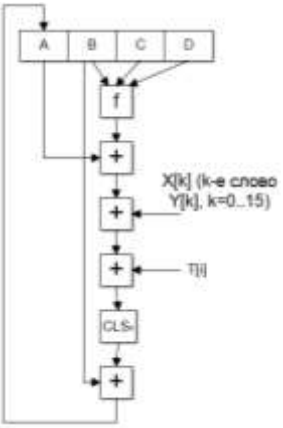

Рисунок 8.8 – Логіка виконання окремого кроку

Кожен із кроків можна подати у такому вигляді:

$$A \leftarrow B+CLS_S(A+f(B,C,D)+X[k]+T[i]),$$

де A, B, C, D – чотири слова буфера (після виконання кожного окремого кроку відбувається циклічний зсув вліво на одне слово);

f – одна із елементарних функцій f_F, f_G, f_H та f_I;

CLS_S – циклічний зсув вліво на s біт 32-бітного аргументу

X[k]-M[q×16+k]-k-е – 32-бітуе слово е q-му 512 блоці повідомлення;

T[i] – і-те 32-бітове слово в матриці T;

+ – додавання за модулем 2^{32}.

На кожному із чотирьох циклів алгоритму використовується одна з чотирьох елементарних логічних функцій. Кожна елементарна функція отримує три 32-бітових слова на вході і на виході створює одне 32-бітове слово. Кожна

функція є множиною побітових логічних операцій, тобто n-ий біт виходу є функцією від n-ого біта трьох входів. Елементарні функції такі:

$$f_F = (B \wedge cC) \vee (B \wedge D); \quad f_G = (B \wedge D) \vee (C \wedge D);$$

$$f_H = B \oplus C \oplus D; \quad f_I = C \oplus (B \wedge \overline{D}).$$

Масив з 32-бітових слів X[0…15] містить значення 512-бітного вхідного блоку, який обробляється в даний момент. Кожен цикл виконується 16 разів, а оскільки кожен блок вхідного повідомлення обробляється в чотирьох циклах, то кожен блок вхідного повідомлення обробляється за схемою (рис. 10.7) 64 рази. Якщо уявити вхідний 512-бітний блок у вигляді шістнадцяти 32-бітових слів, то кожне вхідне 32-бітове слово використовується чотири рази, по одному разу в кожному циклі, і кожен елемент таблиці T, що складається із 64 32-бітних слів, використовується тільки один раз.

Після кожного кроку циклу відбувається циклічний зсув вліво чотирьох слів A, B, C і D. На кожному кроці змінюється тільки одне з чотирьох слів буфера ABCD. Отже, кожне слово буфера змінюється 16 разів, і потім 17-ий раз у кінці для отримання остаточного виходу даного блоку. Додавання алгоритмом можна виконувати наступним чином:

$$MD_0 = IV;$$

$$MD_{q+1} = MD_q + f_I[Y_q, f_H[Y_q, f_G[Y_q, f_F[Y_q, MD_q]]]];$$

$$MD = MD_{L-1},$$

де IV – початкове значення буфера ABCD, визначене на кроці 3;

qY – g-ий 512-бітний блок повідомлення;

L – кількість блоків у повідомленні (включаючи поля доповнення та довжини).

8.3 Алгоритми сімейства SHA

Геш-функція SHA-1. Алгоритм SHA-1 розроблено у 1992 році та формує за вхідним двійковим рядком довільної довжини 160-бітний геш-код. Алгоритм носить циклічний характер і у своїх циклах використовує наступний набір нелінійних функцій:

$$f(u, v, w) = (u \wedge v) \vee (\overline{u} \wedge w);$$

$$g(u, v, w) = (u \wedge v) \vee (u \wedge w) \vee (v \wedge w);$$

$$h(u, v, w) = u \oplus v \oplus w,$$

де u, v,w – 32-бітні змінні (слова);

$u \wedge v$ – логічне «І» за розрядами;

$u \vee w$ – логічне «АБО» за розрядами;

$\overline{u}$ – логічне «доповнення» за розрядами;

$\oplus$ – додавання за модулем 2.

Далі при описі роботи алгоритму символ «+» позначає додавання за модулем 2^{32}, «<<<s» – циклічний зсув уліво на s розрядів.

SHA-1 реалізує геш-функцію, побудовану на ідеї функції стиснення. Входами функції стиснення є блок повідомлення довжиною 512 біт і вихід попереднього блоку повідомлення. Вихід є значення всіх геш-блоків до цього моменту. Іншими словами геш-блок M_I дорівнює $h_i=f(M_i, h_{i-1})$. Геш-значенням всього повідомлення є вихід останнього блоку.

Алгоритм SHA-1. Вхід: двійковий рядок x довжиною 0≥b. Вихід: 160-бітний геш-код за рядком x.

1. Ініціалізація. Ініціалізувати п’ять векторів ініціалізації:

$h_1=67452301_x$; $h_2=efcdab89_x$; $h_3=98badcfe_x$; $h_4=10325476_x$; $h_5=c3d2e1f0_x$.

Задати чотири додаткові константи:

$$y_1=5a827999_x;\ y_2=6ed9eba1_x;\ y_3=8f1bbcdc_x;\ y_4=ca62c1d6_x.$$

2. Передобробка. Доповнити рядок x так, щоб його довжина була кратна числу 512. Для цього необхідно додати в кінець рядка одиницю, а потім стільки ж нульових біт, скільки буде необхідно для отримання рядка довжиною на 64 біти коротшим за довжину, яка кратна 512. Додати останні два 32-х розрядні слова, що містять двійкове представлення числа b. Нехай m – кількість 512-бітних блоків в отриманому доповненому рядку. Таким чином, форматований вхід буде складатися з 16^m 32-х розрядних слів $x_0, x_1, \ldots, x_{16m-1}$. Ініціалізуємо вектор змінних зчеплень:

$$(H_1, H_2, H_3, H_4, H_5)=(h_1, h_2, h_3, h_4, h_5).$$

3. Обробка. Для всіх і від 0 до m-1 кожний і-й блок із шістнадцяти 32-х бітних слів слід перетворити у вісімдесят 32-х бітних слів та записати у тимчасовий масив за наступним алгоритмом:

$$X_i=x_{16i+j}\ (0\le j\le 15);$$

$$X_i = \left(\left(X_{j-3} \oplus X_{j-8} \oplus X_{j-14} \oplus X_{j-16}\right)<<<1\right).$$

Зазначимо, що у початковій версії, яку названо SHA, алгоритм не містить лівого зрушення на один біт. Ця зміна введена для посилення геш-функції. У результаті отриманий алгоритм SHA-1.

Ініціалізування робочих змінних:

$$(A, B, C, D, E)=(H_1, H_2, H_3, H_4, H_5).$$

Обчислення для усіх і від 0 до m-1:

– для j=0 до 19

$$t=((A<<<5)+f(B, C, D)+E+X_j+y_1);$$

$$(A, B, C, D, E)=(t, A, B<<<30, C, D);$$

– для j=20 до 39

$$t=((A<<<5)+h(B, C, D)+E+X_j+y_2);$$

$$(A, B, C, D, E)=(t, A, B<<<30, C, D);$$

– для j=40 до 59

$$t=((A<<<5)+g(B, C, D)+E+X_j+y_3);$$

$$(A, B, C, D, E)=(t, A, B<<<30, C, D).$$

Обновлення вектора змінних зчеплень:

$$(H_1, H_2, H_3, H_4, H_5)\ (H_1+A, H_2+B, H_1+C, H_4+D, H_5+E).$$

4. Завершення. За геш-код приймаємо наступну величину:

$$H_1||H_2||H_3||H_4||H_5.$$

Порівняно із 128-розрядними геш-функціями, 160-розрядний геш-код, який виробляється SHA-1, забезпечує більшу стійкість до силових атак. Геш-функції SHA-1 і RIPEMD-160 за стійкістю приблизно рівні та обидва кращі за MD5.

Розширення блоку вхідного повідомлення введено з метою забезпечення більшої відмінності між вхідними блоками. Надмірність, що вводиться, сприяє підвищенню стійкості геш-функції. На рисунку 8.9 наведено схему однієї ітерації алгоритму SHA-1.

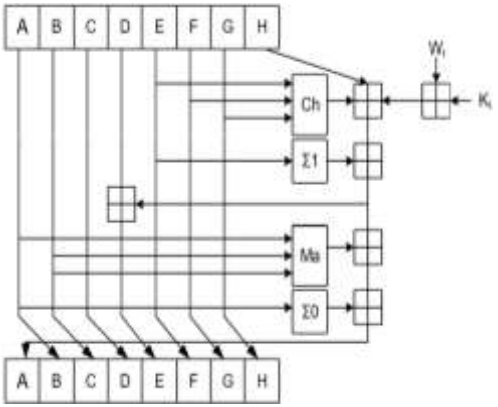

Рисунок 8.9 – Одна ітерація алгоритму SHA1

Геш-функція SHA-2. Secure Hash Algorithm Version 2 – безпечний алгоритм гешування, версія 2 – збірна назва односпрямованих геш-функцій SHA-224, SHA-256, SHA-384 і SHA-512.

Геш-функції призначені для створення «відбитків» або «дайджестів» повідомлень довільної бітової довжини. Застосовуються в різних додатках або компонентах, пов'язаних із захистом інформації.

Геш-функції SHA-2 розроблені Агентством національної безпеки США і опубліковані Національним інститутом стандартів й технологій у федеральному стандарті обробки інформації FIPS PUB 180-2 в серпні 2002 року. У цей стандарт також увійшла геш-функція SHA-1, розроблена в 1995 році. У лютому 2004 року в FIPS PUB 180-2 була додана SHA-224. У жовтні 2008 року вийшла нова редакція стандарту – FIPS PUB 180-3.

У липні 2006 року з'явився стандарт RFC 4634 «Безпечні гешалгоритми США (SHA і HMAC-SHA)», що описує SHA-1 і сімейство SHA-2. Агентство національної безпеки від імені держави випустило патент на SHA-2 під ліцензією Royalty Free.

Загальний опис. Геш-функції сімейства SHA-2 побудовані на основі структури Меркле-Дамгарда.

Початкове повідомлення після доповнення розбивається на блоки, кожен блок – на 8 слів. Алгоритм пропускає кожен блок повідомлення через цикл з 64-ма чи 80-ма ітераціями (раундами). На кожній ітерації 2 слова з восьми перетворюються, функцію перетворення задають інші слова. Результати обробки кожного блоку складаються, сума є значенням геш-функції.

Алгоритм використовує такі бітові операції:

- «||» – конкатенація;
- «+» – додавання;
- «AND» – побітове «І»;
- «OR» – побітове «АБО»;
- «XOR» – виключає «АБО»;
- «SHR» – логічний зсув вправо;
- «ROTR» – циклічний зсув вправо.

На рисунку 8.10 подано схему однієї ітерації алгоритму SHA-2, а у таблиці 8.4 – деякі технічні характеристики різних варіантів SHA-2.

«Внутрішній стан» означає проміжну геш-суму після оброблення чергового блоку даних.

Геш-функції SHA-2 використовуються для перевірки цілісності даних і в різних криптографічних схемах.

На сьогодні сімейство гешфункцій SHA-2 не має такого широкого розповсюдження, як MD5 і SHA-1 незважаючи на виявлені в останніх недоліки.

Алгоритми гешування SHA-3. Основними вимогами, які були висунуті

Національним інститутом стандартів і технологій США (NIST) до алгоритмів-конкурсантів, припускають створення класу геш-функцій потенційно стійких до атак, націлених на SHA-2, а також збереження або збільшення ефективності гешування порівняно з SHA-2.

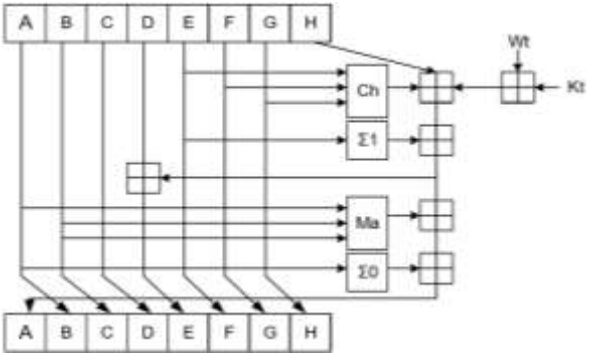

Рисунок 10.10 – Схема однієї ітерації алгоритмів SHA-2

Таблиця 10.4 – Характеристики SHA-2

Геш-функція	Довжина дайджесту повідомлення (біт)	Довжина внутрішнього стану (біт)	Довжина блоку (біт)	Максимальна довжина повідомлення (біт)	Довжина слова (біт)	Кількість ітерацій в циклі
SHA256/224	256/224	256	512	$2^{64}…1$	32	64
SHA512/384	512/384	512	1024	$2^{128}…1$	64	80

Алгоритм-переможець конкурсу SHA-3 має підтримувати розмір вихідного блоку 224, 256, 384 і 512 бітів. Використання дайджестів геш-кодів довжиною 160-біт не допускаються через можливість знаходження колізій атаками грубої сили (повного перебору всіх варіантів). При проведенні конкурсу зберігаються ті ж вимоги, що і до попередніх геш-функцій: максимальний розмір вхідного значення, розмір вихідного значення, колізійна стійкість, стійкість до знаходження прообразу і другого прообразу, потоковий режим обчислення «за один прохід».

Алгоритми функцій обчислення для різного розміру блоків повинні бути ідентичні й мати мінімум відмінностей під час реалізації. Використання

абсолютно різних наборів алгоритмів для отримання чотирьох фіксованих значень довжини виходу не допускається.

Окрім цього висуваються вимоги щодо удосконалення існуючих алгоритмів роботи геш-функцій: можливо включення опції рандомізованого гешування, покращене розпаралелювання, оптимальна робота на безлічі сучасних платформ (включаючи як 64-бітові процесори, так і 8бітові процесори, а також смарт-карти).

Під час конкурсу було допущено використання параметризації в алгоритмах-конкурсантів – зміна параметрів числа раундів з урахуванням допустимих меж «ефективності в обмін на безпеку» (хоча у стандарт ця можливість не включена).

У геш-функції класу SHA-3 можуть бути вбудовані процедури погодження для обчислення кодів автентифікації повідомлень (HMAC): наприклад, передача в якості одного з вхідних параметрів довжини блоку вхідного повідомлення, якщо вона заздалегідь точно відома. Значення всіх вбудованих параметрів і констант повинні бути сконструйовані таким чином, щоб не дати можливості вбудовування лазівок і відмичок з боку розробників, для чого мають бути приведені відповідні докази та процедури перевірки.

Аналіз специфічних вимог до стійкості дозволяє зробити висновок, що основною вимогою є забезпечення теоретичних меж стійкості (в реальності вони можуть бути трохи меншими) на розмір вихідної блоку в n біт і становитиме:

– в конструкціях кодів автентифікації повідомлень (HMAC) і псевдовипадкових функцій (PRF) стійкість за кількістю запитів повинна бути не менше 2(n/2) біт проти атак-розрізнювачів;

– стійкість рандомізованого гешування проти атаки знаходження $H(M_1, r_1)=H(M_2, r_2)$ – не менше n біт, за умови, що значення рандомізатора r_1 не контролюється атакуючим.

Стандартні та додаткові параметри стійкості:

– стійкість до знаходження колізій – не менше n/2 біт;

– стійкість до знаходження прообразу – n біт;

– стійкість до знаходження другого прообразу – n-k бітів для будь-якого повідомлення, коротше 2k бітів;

– стійкість до атак на зміну довжини повідомлення;

– підмножина геш-функцій (наприклад, отримане усіканням числа бітів виходу) розміром m бітів повинно зберігати властивості n-бітного множини в перерахунку на m, з урахуванням статистичних (не відрізняються від випадкових) відхилень.

Не повинно існувати атаки на швидке знаходження малостійких підмножин геш-функції з вихідної множини n; стійкість до нових типів атак, наприклад, на основі мультиколізій. Національним інститутом стандартів і технологій США 29 березня 2012 року був проведений третій раунд конкурсу SHA-3 (у таблиці 8.5 наведено основні характеристики алгоритмів-претендентів).

Аналіз наведеної таблиці показує, що основну увагу розробників алгоритмів-конкурсантів було направлено на виконання основних вимог щодо продуктивності та можливості оптимальної роботи алгоритму при його реалізації на безлічі сучасних платформ. Разом з тим керівники конкурсу при відборі алгоритмів-кандидатів у другий тур звернули увагу на стійкість даних алгоритмів до різних видів атак.

Таблиця 8.5 – Характеристики алгоритмів гешування кандидатів

Назва алгоритму	Платформа	Стійкість алгоритму	Швидкодія (Мбіт/с)
BLAKE	8, 32, 64	є достатньо стійким	44,37
Gröstl		нестійкий до атак «напіввільний початок»	7,98
JH	8, 32, 64	низький алгебраїчний ступінь у висновках функції стиснення	10,6
Keccak	32, 64	кількість раундів, необхідна для захисту від атак – 18	8,05
Skein	8, 32, 64	захищений від атак – підбір подовжених повідомлень і псевдо колізій	39,23

У третьому раунді було відібрано алгоритми гешування, в яких не була порушена будь-яким чином безпека. У деяких випадках, представлений варіант був занадто повільним або вимагав занадто багато пам’яті, але NIST вважає, що в деяких випадках, настроюються параметри можуть бути відкоректовані, щоб дати прийнятний рівень продуктивності без шкоди для безпеки.

Попереднє вивчення алгоритмів-учасників показало, що кожен з них запозичив деякі принципи побудови у алгоритму AES для забезпечення стійкості геш-кодів.

Таким чином, головною вимогою до алгоритмів-конкурсантів керівники NIST висунули безпеку, що і стало основним критерієм відбору кандидатів у третьому раунді.

Варто зауважити, що лише 5 алгоритмів із 14, які було відібрано після другого раунду (всього на конкурс було подано 51 алгоритм) змогли продемонструвати необхідний рівень захисту від криптографічних атак. До основних критеріїв відбору також відноситься продуктивність і можливість роботи на великому числі платформ, що також дозволило керівникам конкурсу «відсіяти» кілька кандидатів (алгоритми Vortex, LUX тощо).

BLAKE (Jean-PhilippeAumasson). BLAKE – є алгоритмом стиснення, функція якого заснована на використанні ключової підстановки в конструкції Davies-Meyer. Ключова підстановка заснована на внутрішній організації потокового шифру ChaCha. Отримав свою не лінійність з накладенням модульного складання і операцій XOR. Сама інноваційна частина BLAKE – своя ключова перестановка.

Структурну схему алгоритму наведено на рисунку 8.11.

Рисунок 8.11 – Структурна схема алгоритму BLAKE

Геш-функція BLAKE-32 працює з 32-бітними словами й повертає 32-байтовое значення геша. Цей відрізок визначає BLAKE-32, виходячи з постійних параметрів власної функції стиску, а потім переходить до його ітеративного режиму.

Константи. BLAKE-32 запускає гешування від того ж початкового значення, що й SHA-256:

IV_0=6A09E667; IV_1=; IV_2=3C6EF372; IV_3=A54FF53A; IV_4=510E527F; IV_5=9B05688C; IV_6=1F83D9AB; IV_7=5BE0CD19.

BLAKE-32 використовує 16 сталих значень:

c_0=243F6A88; c_1=85A308D3; c_2=13198A2E; c_3=03707344; c_4=A4093822; c_5=299F31D0; c_6=082EFA98; c_7=EC4E6C89; c_8=452821E6; c_9=38D01377; c_{10}=BE5466CF; c_{11}=34E90C6C; c_{12}=C0AC29B7; c_{13}=C97C50DD; c_{14}=3F84D5B5; c_{15}=B5470917.

Десять перестановок {0, ..., 15}, які використовуються усіма функціями BLAKE, наведено у таблиці 8.6.

Функція стискання. На вході в BLAKE-32 ця функція має чотири значення:

– ланцюгове значення h=h_0, ..., h_7;

– блок повідомлення $m=m_0, ..., m_{15}$;
– сіль (модифікатор) $s=s_0, ..., s_3$;
– лічильник $t=t_0, t_1$.

Таблиця 8.6 – Перестановки {0, ..., 15}, які використовуються функціями BLAKE

σ_0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
σ_1	14	11	4	8	9	15	13	6	1	12	0	2	11	7	5	3
σ_2	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
σ_3	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
σ_4	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
σ_5	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
σ_6	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
σ_7	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
σ_8	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
σ_9	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0

Ці чотири входи в підсумку є 30-ма словами (тобто, 120 байт=960 біт). На виході функції – нове ланцюгове значення $h'=h_0', ..., h_7'$ з восьми слів (тобто, 32 байта=256 біт). Записуємо стискання h, m, s, t в h' як $h'=compress(h, m, s, t)$.

Ініціалізація. Стан 16-слова $v_0, ..., v_{15}$ ініціалізовано так, що різні входи виробляють різні початкові стани. Стан представляється як матриця розміром 4×4, і заповнюється так, як зазначено далі:

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \leftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus c_4 & t_0 \oplus c_5 & t_1 \oplus c_6 & t_1 \oplus c_7 \end{pmatrix}.$$

Циклічна функція. Як тільки стан v проініціалізовано, функція стискання виконує ітерації серіями по 10 раундів. Раунд – це перетворення значення v, яке обчислюється:

$$G_0(v_0, v_4, v_8, v_{12}); G_1(v_1, v_5, v_9, v_{13}); G_2(v_2, v_6, v_{10}, v_{14}); G_3(v_3, v_7, v_{11}, v_{15});$$
$$G_4(v_0, v_5, v_{10}, v_{15}); G_5(v_1, v_6, v_{11}, v_{12}); G_6(v_2, v_7, v_8, v_{13}); G_7(v_3, v_4, v_9, v_{14}),$$

де r – раунд;

$G_i(a, b, c, d)$ – множини.

$$a \leftarrow a + b + \left(m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)}\right);\ \ d \leftarrow (d \oplus a) <<< 16;$$
$$c \leftarrow c + d;\ \ b \leftarrow (b \oplus c) <<< 12;$$
$$a \leftarrow a + b + \left(m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)}\right);\ \ d \leftarrow (d \oplus a) <<< 8;$$
$$c \leftarrow c + d;\ \ b\, b \leftarrow (b \oplus c) <<< 7.$$

Перші чотири виклики G_0, …, G_3 можуть бути розраховані паралельно, тому що кожен з них обновляє окремий стовпець матриці. Необхідно звернутися до процедури обчислення G_0, …, G_3 крок стовпець. Так само останні чотири виклики G_4, …, G_7 обновлюють певні діагоналі й таким чином можуть бути синхронізовані таким чином, що необхідно звертатися до діагонального кроку.

На рисунках 8.12 і 8.13 наведено G_i, крок-стовпець і діагональний крок.

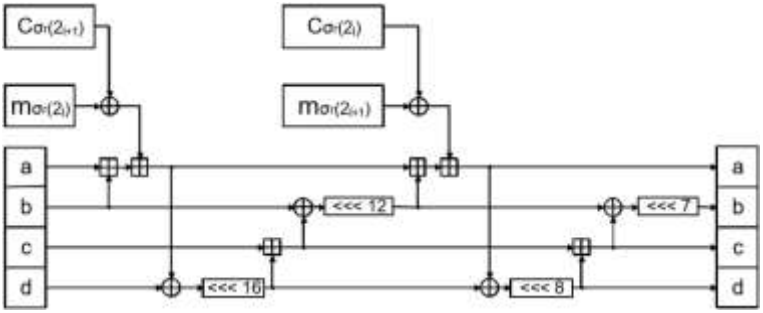

Рисунок 8.12 – Функція G_i

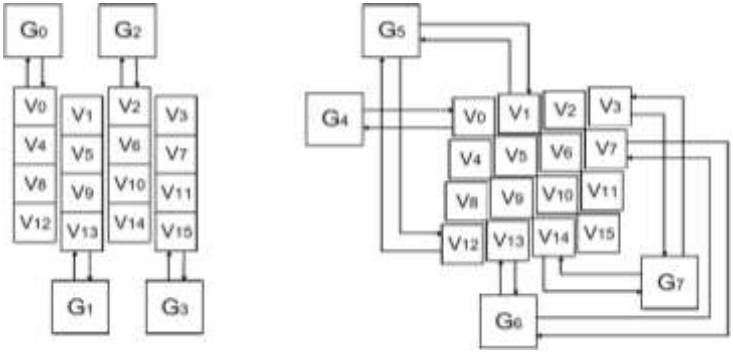

Рисунок 8.13 – Крок-стовпець і діагональний крок

Завершення. Після послідовності циклів нове ланцюгове значення h_0', ..., h_7' отримується із встановленого v_0, …, v_{15} із входом початкового ланцюгового значення h_0, …, h_7 і солі s_0, …, s_3:

$$h_0' \leftarrow h_0 \oplus s_0 \oplus v_0 \oplus v_8;\ \ h_1' \leftarrow h_1 \oplus s_1 \oplus v_1 \oplus v_9;$$
$$h_2' \leftarrow h_2 \oplus s_2 \oplus v_2 \oplus v_{10};\ \ h_3' \leftarrow h_3 \oplus s_3 \oplus v_3 \oplus v_{11};$$
$$h_4' \leftarrow h_4 \oplus s_4 \oplus v_4 \oplus v_{12};\ \ h_5' \leftarrow h_5 \oplus s_5 \oplus v_5 \oplus v_{13};$$
$$h_6' \leftarrow h_6 \oplus s_6 \oplus v_6 \oplus v_{14};\ \ h_7' \leftarrow h_7 \oplus s_7 \oplus v_7 \oplus v_{15}.$$

Гешування повідомлення. Процедура для гешування повідомлення m розрядної довжини l<264 притаманна циклічним геш-функціям, повідомлення спочатку доповнюється: при додаванні BLAKE використовує правило, подібне до правила HAIFA, потім оброблений блок пріймається функцією стискання.

Доповнення. Спочатку повідомлення розширюють таким чином, що його довжина збігається із 447 за модулем 512. Довжина збільшується, додаючи в кінець достатню кількість 0 біт. Збільшення як мінімум на один біт, і як максимум на 512. Потім приєднується одиничний біт, за ним іде 64-бітне невизначене багатобайтове подання l. Доповнення може бути поданим, як:

$$m \leftarrow m\|1000\ldots0001(I)_{64}.$$

Ця процедура гарантує, що бітова довжина повідомлення, яка доповнюється, кратна 512.

Гешування. Щоб приступити до гешування, доповнене повідомлення розбивають на блоки по 16-ть слів m_0, …, m_{n-1}. Нехай l_i кількість біт у повідомленні m_0, …, m_i, тобто окрім бітів, доданих під час доповнення. Наприклад, якщо оригінальне (не доповнене) повідомлення 600-біт у довжину, то доповнене повідомлення буде мати два блоки: l_0=512 та l_1=600. Окремий випадок відбувається, коли останній блок не містить жодного біта оригінального повідомлення; наприклад 1020-розрядне повідомлення приводить до доповненого повідомлення із трьома блоками (які містять відповідно 512, 508, і 0 біт повідомлення), і треба встановити l_0=512, l_1=1020, l_2=0. Загальне правило: якщо останній блок не містить жодного біта оригінального повідомлення, тоді лічильник зводиться до нуля; це гарантує, що, якщо $i \neq j$, то $l_i \neq l_j$.

Сіль s вибирається користувачем, і встановлюється нульовою, у тому випадку коли її не потрібно (тобто, $s_0=s_1=s_2=s_3=0$). Гешування доповненого повідомлення m проводиться, за наступним прикладом:

$h_0 \leftarrow IV;$
fori=0, …, N-1;
$h^{i+1} \leftarrow compress(h^i, m^i, s, l^i);$
$returnh^N.$

Процедура гешування m з BLAKE-32 записується у наступному вигляді:

$$BLAKE\text{-}32(m, s)=h_n,$$

де m –повідомлення (не доповнене);

s – сіль.

Запис BLAKE-32(m) означає гешування m, за умови, що жодна сіль не використовується (тобто, s=0).

Регульований параметр. Під час його виклику для нової геш-функції NIST сприяє опису параметра, який допускає швидкість/довіру вибору оптимального розв'язку. Для BLAKE цей параметр – кількість циклів. Мінімальна кількість раундів для BLAKE-32 та BLAKE-28 – 5, а для BLAKE-64 і BLAKE-48 – 7.

Grostl (LarsRamkildKnudsen). Grostl – колекція геш-функцій, здатних повертати короткі виклади повідомлень будь-якої кількості байтів від 1 до 64, тобто від 8 до 512 біт у 8 бітних кроках.

Різновиди, що повертають n біт називаються Grostl-n. Це включає розміри короткого викладу повідомлення 224, 256, 384, і 512 біт.

Конструкція геш-функції. Геш-функції Grostl повторюють функцію стиску f таким чином. Повідомлення M доповнене й розділене на блоки повідомлення по l біт m_1, ..., m_t, і кожний блок повідомлення обробляється послідовно.

Початкове l-бітне значення h_0=iv визначене, а згодом блоки повідомлень m_i обробляють за виразом:

$$h_i \leftarrow (h_{i-1}, m_i), \text{ for } i=1, \ldots, t.$$

Отже, в картах два входи по l біт кожний і вихід з l біт. Перший вхід прийнято називати послідовним входом, а другий вхід – блок повідомлення.

Різновиди Grostl повертають аж до 256 біт, l визначено як 512. Для більших різновидів, l – 1024. Після того, як останній блок повідомлення був оброблений, вихід геш-функції H(M) обчислюють за виразом:

$$H(M)=\Omega\,(ht),$$

де Ω – вихідне перетворення.

Вихідний розмір Ω – n біт, тому варто зазначити, що n<l. Струткту геш-функції наведено на рисунку 8.14.

Конструкція функції стискання. Функція стискання заснована на двох основних l-бітних перестановках P і Q, які зазвичай визначають у наступний спосіб:

$$f(h,\ m) = P(h \oplus m) \oplus Q(m) \oplus h.$$

Рисунок 8.14 – Геш-функція Grostl

На рисунку 8.15 наведено конструкцію функції стискання f.

Вихідне перетворення. Нехай truncn(x) є операцією, яка відкидає всі майже кінцеві n біти x. Після цього вихідне перетворення (рис. 8.16) визначається, як:

$$\Omega(x)=\text{truncn}(P(x)\oplus x).$$

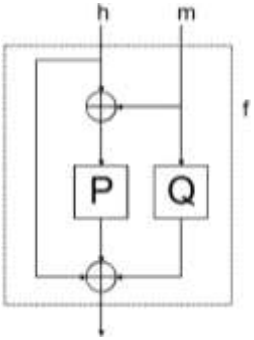

Рисунок 8.15 – Функція стискання f (P і Q – l-бітні перестановки)

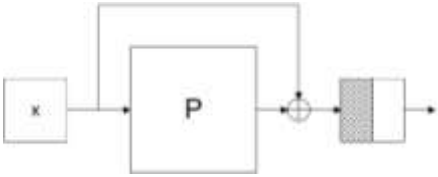

Рисунок 8.16 – Вихідне перетворення Ω

Тобто вихідне перетворення Ω розраховується як $P(x)\oplus x$, після чого виключає вихід, повертаючи тільки останні n біт.

Проектування від байтової послідовності до встановленої матриці й навпаки. Оскільки Grostl оперує байтами, а це в основному невизначені байти. Однак, необхідно конкретизувати, як саме байтова послідовність проектується на матрицю A і навпаки. Цей розподіл зроблений аналогічним способом як в Rijndael. Отже, 64-байтова послідовність 00 01 02...3f відображається як матриця 8×8.

$$\begin{bmatrix} 00 & 08 & 10 & 18 & 20 & 28 & 30 & 38 \\ 01 & 09 & 11 & 19 & 21 & 29 & 31 & 39 \\ 02 & 0a & 12 & 1a & 22 & 2a & 32 & 3a \\ 03 & 0b & 13 & 1b & 23 & 2b & 33 & 3b \\ 04 & 0c & 14 & 1c & 24 & 2c & 34 & 3c \\ 05 & 0d & 15 & 1d & 25 & 2d & 35 & 3d \\ 06 & 0e & 16 & 1e & 26 & 2e & 36 & 3e \\ 07 & 0f & 17 & 1f & 27 & 2f & 37 & 3f \end{bmatrix}.$$

Для матриці 8×16, цей метод розширюється природним шляхом. Розподіл від матриці до байтової послідовності – просто зворотна операція.

Кількість раундів. Кількість раундів r є регульованим параметром безпеки. У таблиці 8.7 подано рекомендовані величини r для чотирьох перестановок.

Таблиця 8.7 – Рекомендовані для перестановок величини r

Перестановки	Розмір викладу	Рекомендоване значення r
P512 і Q512	8-256	10
P1024 і Q1024	264-512	14

Початкові значення. Початкове значення ivngrostl-n – l-бітне представлення n. У таблиці 8.8 наведено початкові значення, які є необхідними для вихідних розмірів 224, 256, 384, і 512 біт.

Таблиця 8.8 – Початкові значення n

n	ivn
224	00...00 00 e0
256	00...00 01 00
384	00...00 01 80
512	00...00 02 00

Доповнення. Довжина кожного блоку повідомлення – l. Щоб бути здатним подіяти на входи змінної довжини, функція доповнення pad має бути визначеною. Ця функція доповнення приймає рядок x довжиною в N біт і повертає доповнений рядок x*=pad(x) довжиною, яка є кратною l.

Функція, яка доповнює, робить наступні дії. Спочатку вона додає «1» біт до x. Потім вона додає w=–N–65mod l «0» біт, і нарешті вона додає 64- бітне представлення (N+w+65)/l. Це число є цілим через вибір w і представляє кількість блоків повідомлення в кінцевому, доповненому повідомленні.

Оскільки це повідомлення має бути доступним для кодування кількості блоків (в доповненому повідомленні в межах 64 біт) максимальна довжина повідомлення – 65 біт до 2^{64}-1 блоків повідомлення. Для коротких варіантів, максимальна довжина повідомлення в бітах – $512(2^{64}\text{-}1)\text{-}65=2^{73}$–577, і для довших варіантів – це $1024(2^{64}\text{-}1)\text{--}65=2^{74}\text{-}1089$. Початкове значення Grostl-n – l-бітне представлення n.

В остаточному підсумку вихід останнього виклику f обробляється вихідним перетворенням Ω, яке скорочує розмір висновку з l до n бітів.

JH (HongjunWu). JH – використовує нову конструкцію, що дещо нагадує конструкцію «sponge» для вбудовування алгоритму геш у блок-підстановку. Блокпідстановка – це комбінація з двох 4-бітових S-боксу з низкою лінійних операцій змішування і розрядних підстановок. Уся нелінійність у цьому дизайні отримана з S-боксів. Структурну схему алгоритму наведено на рисунку 8.17.

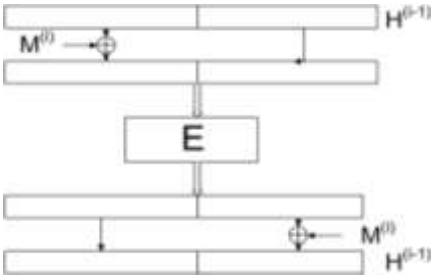

Рисунок 8.17 – Структурна схема алгоритму JH

Keccak (JoanDaemen). Keccak – використовує конструкцію «sponge» і блок-підстановку. Підстановка може бути реалізована на основі 5-бітових S-блоків або на комбінації лінійної і нелінійної операціях змішування. Структурну схему алгоритму подано на рисунку 8.18.

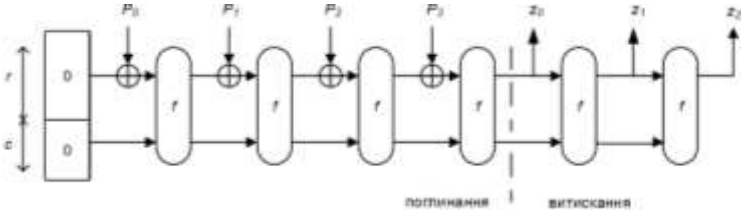

Рисунок 8.18 – Структурна схема алгоритму Keccak

Skein. Skein – це сімейство геш-функцій із трьома різними внутрішньо встановленими розмірами: 256, 512, і 1024 біти.

Skein-512 може безпечно використовуватися для всіх поточних додатків, що гешують та залишається безпечним для найближчого майбутнього.

Skein 1024 притаманний двічі внутрішньо-встановлений розмір – Skein-512. Skein-1024 може працювати вдвічі швидше за Skein-512 у призначених апаратних реалізаціях.

Skein-256. Він може реалізовуватися, використовуючи близько 100 байтів RAM.

Нова ідея Skein полягає у тому, щоб побудувати геш-функцію після використання блокового шифру. Використання стандартного блокового шифру дозволяє Skein гешувати дані конфігурації разом із вхідним текстом у кожному блоці, і зробити будь-яке середовище функції стиску унікальним. Ця властивість безпосередньо адресує множину атак геш-функцій, а також суттєво поліпшує гнучкість Skein.

Точніше кажучи, Skein створений із трьох нових компонентів:

– Threefish – це модифікований блоковий шифр у ядрі Skein, який обмежується 256-, 512- і 1024-бітним розміром блоку;

– Unique Block Iteration (унікальний блок ітерацій, UBI) – режим, який дозволяє підключитись та використовує Threefish, з метою побудови функції стискання, яка перетворює довільний вхідний розмір у фіксований вихідний;

– Optional argument system (додаткова система аргументу) – вона дозволяє Skein підтримувати ряд додаткових характеристик, не вимагаючи, при цьому, ніяких перевантажень під час виконання додатків, які не використовують характеристики.

Основний Threefish алгоритм описує багаторічні знання проектування блокового шифру й аналізу. UBI є безпечним і може використовуватися із будь-якими налагодженими шифрами. Додаткова система аргументу дозволяє Skein пристосовуватися для різних цілей. Ці три компоненти незалежні й можуть використовуватися окремо, але їх комбінація забезпечує реальні переваги.

Гешування Skein. Skein побудований на числених викликах UBI. На рисунку 8.19 наведено Skein, як просту геш-функцію. Починаючи з ланцюгового значення 0, на практиці розрізняють три виклики UBI: за кожним на конфігураційний блок, повідомлення (аж до 2^{96}-1 байт у довжину), і вихідне перетворення.

32-байтовий рядок конфігурації шифрує бажану вихідну довжину й деякі параметри, щоб підтримувати дерево гешування. Якщо Skein використовується як стандартна геш-функція – з фіксованим вихідним розміром і без дерева гешування або MAC ключа – результатом обчислення конфігураційного блоку

UBI є константа для всіх повідомлень і може бути попередньо розрахована як IV.

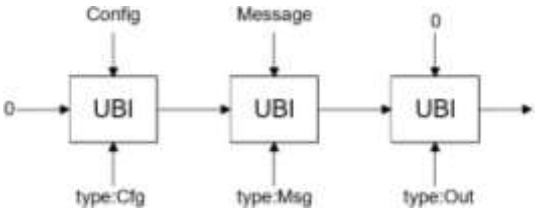

Рисунок 8.19 – Режим нормального гешування Skein

Вихідні перетворення потрібні для досягнення гешування необхідної довільності. Це також дозволяє Skein породжувати виходи будь-якого розміру аж до 264 біт. Якщо одного вихідного блоку недостатньо, вихідні перетворення запускаються декілька разів, як показано на рисунку 8.20. З'єднані входи з усіма вихідними перетвореннями однакові, поле даних складається з 8-байтового лічильника (використовується Threefish у режимі лічильника). Створення більших виходів часто зручно, але звичайно безпека Skein обмежена внутрішньо встановленим розміром.

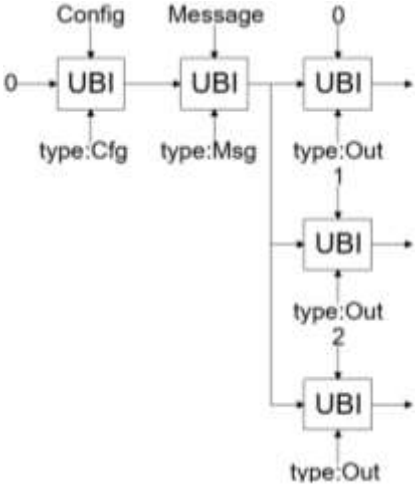

Рисунок 8.20 – Skein із більшим вихідним розміром

Додаткові аргументи. Для того, щоб збільшити гнучкість Skein, кілька додаткових входів можуть бути дозволені, у якості необхідних. Усі ці опції управляються додатками реального часу.

Ключ (додатковий). Ключ, який перетворює Skein у MAC або KDF функцію. Ключ завжди обробляють в першу чергу, щоб підтримувати деякі із доказів безпеки.

Конфігурація (необхідна).

Персоналізація (додаткова). Рядок, який можуть використовувати додатки для створення різних функцій для різного використання.

Відкритий ключ (додатковий). Відкритий ключ використовується при гешуванні повідомлення для його підпису. Це зв'язує геш підпису й відкритий ключ. Таким способом ця характеристика перевіряє те, що одне й теж повідомлення генерує різний геш для різних відкритих ключів.

Ключ ідентифікатор висновку (додатковий). Використовується для добування ключів. Для того, щоб одержати ключ, заготовлюють головний ключ як ключ для входу, і ідентифікатор запитуваного похідного ключа.

Поточний час (додатковий). Поточне значення часу використовується в потокових шифрах і рандомізованому гешуванні.

Повідомлення (додаткове). Нормальне вхідне повідомлення для геш-функції.

Вихідне перетворення. Обчислення Skein складаються із обробки цих опцій у порядку, що використовується UBI. Кожний вхід має різний «тип» значення для модифікації, який гарантує, що входи не взаємозамінні.

Жодне з них не впливає на виконання й складність основної геш-функції жодною мірою; інші реалізації можуть вибирати яку опцію реалізувати, а яку проігнорувати.

Очевидно, Skein може бути розширений з іншими необов'язковими аргументами. Вони можуть бути додані в будь-який час, навіть, коли функція вже була стандартизована, тому що додавання нових необов'язкових аргументів є оборотно-сумісним.

Skein-MAC. Стандартний спосіб використовувати геш-функцію для автентифікації – використовуючи конструкцію HMAC. Skein звичайно ж може бути використаний із HMAC, але це вимагає як мінімум двох геш-обчислень для кожної автентифікації, що є неефективним для коротких повідомлень. Перетворення Skein у MAC наведено на рисунку 8.21.

Замість обробки блоку конфігурації, яка починається з нуля, починається обробка ключа з нуля, а потім вже блоку конфігурації. Або дивлячись з іншого боку, Skein гешування просто Skein-MAC з нульовим ключем. Подібно до того, як вихід Skein конфігураційного блоку попередньо обчислюється для наданого ключа. З того моменту коли найбільш загальні шляхи було застосовано в MAC

для автентифікації численних повідомлень із єдиним ключем, це дозволило збільшити виконання для коротких повідомлень.

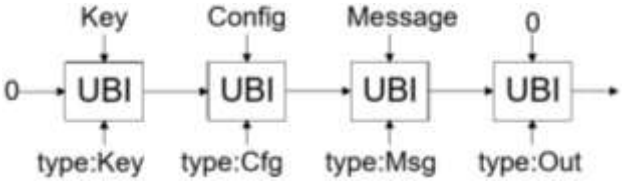

Рисунок 8.21 – Skein-MAC

Дерево гешування. Замість гешування даних як одного великого рядка, вони розділяються на частини. Кожна частина гешується й результуючий геш розглядається як нове повідомлення. Ця процедура може застосовуватися рекурсивно, поки результат не стане єдиним значенням геша.

Skein включає режим гешування деревом для підтримки додатків цього типу. Оскільки різні додатки мають різні вимоги, то ці три параметри для додатка можуть обиратися для конкретного використання додатка: вузловий розмір листа, treefan-out, і максимальна висота дерева.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Гешувальні алгоритми: призначення та вимоги, які висуваються до них.
2. Алгоритми формування кодів-гешування.
3. Безключові геш-функцій.
4. Способи використання кодів цілісності даних в сучасних ІС.
5. MDC- та MAC-коди.
6. Основні переваги алгоритмів гешування.
7. Універсальні класи гешування даних.
8. Каскадні схеми гешування.

Література: [1-17].

ЗМІСТОВНИЙ МОДУЛЬ 2. Апаратні засоби захисту інформації та алгоритм її здійснення

Тема 9. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів її витоку

План:

9.1 Технічний канал витоку інформації

9.2 Загальний підхід до технічного захисту інформації

9.3 Фізичні основи утворення технічних каналів витоку інформації

9.4 Організаційно-технічні заходи щодо ТЗІ на об’єкті

9.5 Основи несанкціонованого зняття інформації способом та засобами високочастотного нав’язування

9.6 Класифікація каналів витоку інформації

9.1 Технічний канал витоку інформації

Технічний захист інформації призначений для захисту інформації від витоку по технічних каналах.

На даний час для несанкціонованого зняття інформації широко використовують технічні канали витоку інформації (ТКВІ). Технічний канал витоку інформації – це сукупність небезпечних фізичних сигналів, середовища їх розповсюдження та зберігання, об’єкту, способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об’єкту, який охороняється.

Небезпечний фізичний сигнал (небезпечний сигнал) – це сигнал, який містить інформацію, яку необхідно захищати.

На практиці ТКВІ класифікують за наступними ознаками:

– акустичні канали витоку інформації (у тому числі канали із акустично-електричними перетвореннями);

– радіотехнічні канали витоку інформації (у тому числі відкриті канали радіотехнічного зв’язку та канали, які утворюються за рахунок паразитних випромінювань та наводок);

– оптичні канали витоку інформації;

– речовий канал витоку інформації (визначається людським чинником).

ТКВІ можуть бути природними та штучними, у тому числі створеними навмисно. Природні ТКВІ утворюються на базі фізичних властивостей джерел виникнення небезпечних сигналів, самих небезпечних сигналів та середовища їх розповсюдження. Для навмисного створення ТКВІ використовуються змінні фізичні властивості джерел та середовищ розповсюдження небезпечних сигналів, а також подачею спеціальних сигналів на окремі елементи приміщення (це зазвичай робиться шляхом конструктивних змін джерел та конструкції об’єкту, де розповсюджуються небезпечні сигнали).

Слід пам’ятати, що для зняття інформації із ТКВІ перевага надається апаратурі технічної розвідки. Окрім цього, така апаратура, за умови її розміщення на об’єкті, який охороняється, утворює навмисний канал витоку інформації.

На рисунку 9.1 подано загальну класифікацію видів інформації, яка може бути об’єктом несанкціонованого доступу.

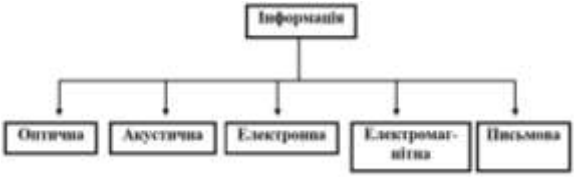

Рисунок 9.1 – Загальна класифікація видів інформації, яка є об’єктом несанкціонованого доступу

Відповідно, усі види інформації (оптична, акустична, електронна, електромагнітна та письмова/друкована) мають різну фізичну природу її походження, носіїв і каналів розповсюдження та зберігання, або різні параметри одного й того ж явища, яке може бути покладене в основу для її перенесення або зберігання.

Зрозуміло, що для проведення робіт із розроблення, впровадження, підтримка та перевірка працездатності системи ТЗІ на об’єкті, який охороняється, вимагає проведення певних організаційно-технічних заходів. А їх проведення призначене, перш за все, для забезпечення надійності захисту інформації на об’єкті.

Одним із найважливіших завдань ТЗІ є виявлення та блокування усіх потенційних каналів витоку інформації з об’єкту. Паралельно з цим відбувається постійна перевірка працездатності та надійності функціонування системи технічного захисту.

9.2 Загальний підхід до технічного захисту інформації

Класична схема оброблення та розповсюдження інформації наведена в теорії інформації та подана на рисунку 9.2. Вона містить передавач інформації, канал зв’язку (або канал зберігання, чи обидва канали разом) інформації, та приймач (який може мати систему вторинної обробки) інформації.

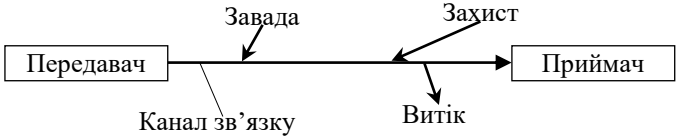

Рисунок 9.2 – Класична схема оброблення, розповсюдження та захисту інформації

З точки зору класичної теорії інформації канал зв'язку є найбільш уразливою ділянкою для дії завад. Це ж правило діє й під час розгляду проблем захисту інформації. Але з позиції захисту інформації канал зв'язку варто розглядати у двох напрямках:

– як канал витоку;

– як ділянку, яка є зручною для захисту.

Варто пам'ятати, що під час розгляду каналів витоку інформації, способів її викрадення та методів блокування не розглядають звичайних способів крадіжки письмової інформації та її носіїв, оскільки це є речовим каналом витоку інформації.

Основними об'єктами захисту інформації прийнято вважати:

– інформаційні ресурси, до складу яких входять відомості, які віднесено до таємної або конфіденційної інформації;

– засоби і системи інформації (програмні засоби (системи управління базами даних, операційні системи тощо), автоматизовані системи управління, системи зв'язку і передачі даних, технічні засоби приймання, передачі та оброблення інформації обмеженого доступу, їх інформативні фізичні поля);

– додаткові технічні засобами й системами (ДТЗС) – системи, які не віднесено до засобів і систем інформатизації, але які розташовуються в приміщеннях, де обробляють конфіденційну інформацію (технічні засоби відкритого телефонного зв'язку, засоби оповіщення, системи пожежної та охоронної сигналізації, радіофікації, годинофікації, електропобутові прилади тощо, а також самі приміщення, які призначенні для оброблення інформації з обмеженим доступом).

Окремі технічні засоби або група технічних засобів, які призначені для оброблення конфіденційної інформації, разом із приміщеннями, де вони розташовуються, формують об'єкт технічних засобів приймання, перероблення, зберігання й передачі інформації (ТЗПІ).

9.3 Фізичні основи утворення технічних каналів витоку інформації

У відповідності до прийнятої класифікації поділу ТКВІ доцільним є розгляд фізичних основ утворення акустичних, радіотехнічних та оптичних каналів.

Насамперед доцільно акцентувати увагу на фізиці формування акустичних каналів витоку інформації, при цьому особливу увагу відводять акустично-електричним перетворенням.

Сама назва каналу витоку інформації свідчить про те, що небезпечними сигналами, які можуть витікати через нього, є акустичні сигнали.

Акустичний сигнал – це механічні коливання часток пружного середовища. Отже, виходячи з цього визначення, можна зробити висновок, що акустичний сигнал може розповсюджуватись у будь-якому пружному середовищі. Єдиним середовищем, у якому розповсюдження такого сигналу неможливе – повний вакуум (відсутні частинки повітря, тобто пружнє середовище відсутнє). Саме це і пояснює можливість проходження акустичних сигналів через елементи будівельних конструкцій (стіни, стелі, підлоги, двері, скло вікон, труби тощо).

Акустичний сигнал сприймається безпосередньо слуховими органами людини та інших живих істот. При цьому людина сприймає акустичні коливання у діапазоні частот від 20 до 20000 Гц. Цей діапазон отримав назву – звуковий діапазон частот.

Нагадаємо, що частоті в 1 Гц відповідає коливання, яке утворює повний період за 1 секунду (рис. 9.3). Отже частота сигналу, це кількість повних періодів коливання за 1 секунду.

Окрім звукового, розрізняють інфразвуковий (від 0 до 20 Гц) та ультразвуковий (вище 20000 Гц) діапазони частот. Ці частоти сприймаєчує більшість тварин, але люди їх не чують.

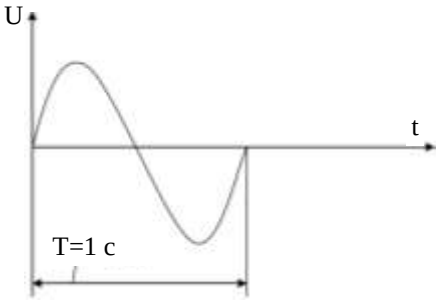

Рисунок 9.3 – Гармонійне коливання з частотою 1 Гц

Для того, щоб передати звук по каналах зв’язку або запам’ятати у приладах звукозапису, акустичний сигнал необхідно перетворити у адекватний йому електричний сигнал. Для такого перетворення використовується спеціальний перетворювач – мікрофон. Для зворотного перетворення використовується гучномовці. Принцип перетворення акустичного сигналу в електричний показано на прикладі вугільного мікрофону (рис. 9.4).

В основу роботи мікрофона покладено ефект зміни електричного опору вугільного порошку під дією механічного тиску акустичних коливань на мембрану мікрофону.

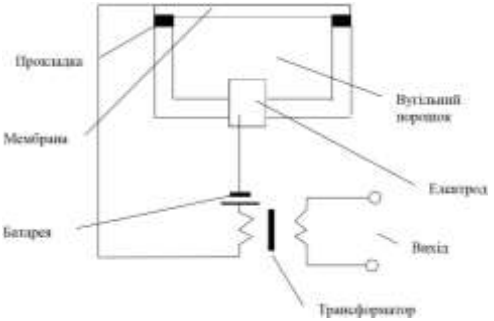

Рисунок 9.4 – Будова вугільного мікрофону

В основу роботи мікрофона покладено ефект зміни електричного опору вугільного порошку під дією механічного тиску акустичних коливань на мембрану мікрофону.

Конструктивно мікрофон являє собою круглу циліндричну металеву коробку із засипаним в неї вугільним порошком. На верхній частині циліндра розташовано діелектрична пружна прокладка, на якій зверху знаходиться мембрана. Конструкція затягується кришкою.

До циліндру з порошком та мембрани підведено два різних полюси джерела постійного струму (батарея). Оскільки вугільний порошок проводить електричний струм, то через первинну обмотку трансформатору протікає постійний струм. Але під дією звукових коливань мембрана стискує порошок, що призводить до зміни його опору. Завдяки цьому у струмі, який протікає у замкнутому ланцюзі, виникає змінна складова, яка передається через підвищувальний трансформатор. Частота і рівень сигналів змінної складової еквівалентні частоті та рівню звукових коливань, які потрапляють на мембрану мікрофона.

Вугільний мікрофон є найпростішим мікрофоном із найгіршими характеристиками перетворення. Така конструкція (вугільний мікрофон є першим типом мікрофонів, які створило людство) здатна вносити найбільші спотворення у перетворювальні сигнали. На сьогодні широко використовують динамічні, конденсаторні та електретні мікрофони, які є обов'язковою складовою усіх засобів зняття акустичної інформації.

Багато інших елементів різних електричних та електронних приладів можуть бути використані для зняття акустичної інформації за рахунок акустоелектричних перетворень, які виникають за рахунок так званого «мікрофонного ефекту».

Принцип його виникнення можна пояснити на прикладі звичайного телефону. Відомо, що на телефон від лінії подається постійний струм з напругою 45 В. Також відомо, що у вхідному каскаді телефону завжди є трансформатор, який підключено до цієї ж лінії. Сам телефон знаходиться у середовищі повітря, отже на трансформатор діє акустичні сигнали розмов, які відбуваються у приміщенні, де цей телефон і знаходиться. При цьому по телефону у цей час розмови не ведуться. Але акустичні хвилі тиснуть на феритовий сердечник трансформатора, що викликає у ньому появу змінного магнітного поля, яке виникає завдяки явищу магнітострикції.

Поява змінного магнітного поля призводить до виникнення змінного струму в обмотках трансформатора за рахунок явища самоіндукції у відповідності до законів Фарадея та Ленца. А цей струм можна зняти безпосередньо з телефонної лінії, підключеної до телефонного апарату. Окрім того, акустичні хвилі тиснуть на обмотки трансформатора, що викликає у них зміну величини паразитної міжвиткової ємності. Це, у свою чергу, призводять до зміни власної резонансної частоти обмоток трансформатора. Такі ж ефекти виникають під час дії акустичного сигналу на будь-які котушки індуктивності.

Варто пам'ятати, що уникнути паразитної міжвиткової ємності та власної резонансної частоти у індуктивностях неможливо, оскільки вони є фізичними властивостями таких елементів.

Всі ці зміни відбуваються із частотою акустичного сигналу, який діє на згадані елементи, та пропорційно рівню його тиску.

Отже, усі розмови в приміщенні можна зняти користуючись «мікрофонним ефектом» та ефектом зміни власної резонансної частоти, які виникають на трансформаторах або котушках індуктивності будь-якого ДТЗС.

Приклад формування змінного струму в обмотках трансформатора телефону подано на рисунку 9.5.

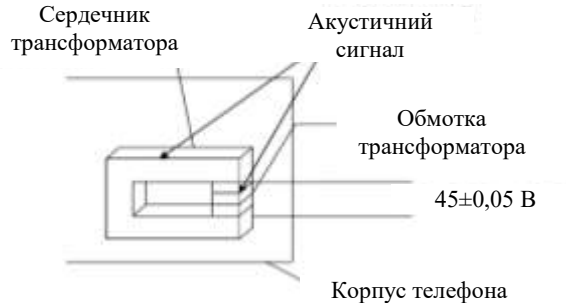

Рисунок 9.5 – Механічна дія акустичного сигналу на трансформатор телефону

Зрозуміло, що для зняття інформації із використанням наведених ефектів необхідно користуватися спеціальною апаратурою для технічної розвідки.

Відкриті канали радіозв'язку. Головною особливістю радіозв'язку є використання процесу модуляції для передавання інформаційних (корисних) сигналів. Його суть полягає у тому, що для переносу на відстань корисного сигналу використовується сигнал-переносник, на який «садять» інформаційний сигнал. Процес реалізується перемноженням цих двох сигналів. У результаті процесу модуляції утворюються модульовані сигнали, які й випромінюються в ефір. Процес модуляції застосовується для забезпечення передавання низькочастотних інформаційних сигналів з найменшими енергетичними затратами, оскільки високочастотні сигнали-переносники для свого випромінювання та розповсюдження вимагають набагато менших енергетичних витрат, ніж низькочастотні.

Сигнал-переносник називають сигналом, який модулюється (несучий сигнал або коливання), а інформаційний сигнал – модулюючим сигналом.

Частота несучого коливання завжди є більшою у порівнянні із частотою інформаційного сигналу.

На практиці розрізняють наступні види модуляції: амплітудна, частотна та фазова.

При амплітудній модуляції інформаційний сигнал у модульованому коливанні проявляється у зміні амплітуди несучого коливання, при частотній – у змінах частоти, при фазовій – у змінах фази.

З переходом на цифрові методи зв'язку використовується й амплітудноімпульсна модуляція, але вона застосовується лише при перетвореннях безперервних сигналів у цифрові та не використовується при випромінюванні радіосигналів у ефір.

Припустимо, що інформаційний сигнал визначається функцією:

$$s_1(t)=A_m \sin\Omega t,$$

а сигнал-переносник функцією:

$$s_2(t)=B_m \cos\omega t,$$

тоді модульований сигнал записується як:

$$s_M(t) = A_m \sin\Omega i \cdot B_m \cos\omega o = \frac{A_m B_m}{2}\left[\sin(\Omega+\omega)t + \sin(\Omega-\omega)t\right],$$

де Ω – частота інформаційного сигналу;

ω – частота сигналу-переносника;

A_m – амплітуда інформаційного сигналу;

B_m – амплітуда сигналу-переносника.

Таким чином, у модульованому коливанні присутні усі компоненти інформаційного сигналу, які можна виділити у процесі демодуляції.

Фізичні основи каналів витоку, які утворюються за рахунок паразитних випромінювань та наводок. Будь-який електронний прилад генерує паразитне випромінювання переважно на власній, індивідуальній, частоті. Це явище супроводжується численними паразитними ємнісними зв'язками, які зазвичай утворюються між провідниками, друкованими струмопроводами, ніжками електрорадіоелементів тощо. При цьому виникають нові паразитні ланцюги, появу яких, під час проектування приладів та у процесі їх виробництва, передбачити неможливо. Такі паразитні ланцюги призводять до появи паразитних позитивних зворотних зв'язків, які й перетворюють будь-який, навіть низькочастотний, електронний прилад (підсилювач) у передавач, який випромінює в ефір паразитні коливання на високих та надвисоких частотах.

Під час проектування та виробництва більшості побутових приладів на такі випромінювання не звертають уваги, оскільки вони не впливають на виконання апаратами своїх функцій. Лише при проектуванні та виробництві спеціальної та захищеної апаратури для цих параметрів приділяють неабияку увага.

Оскільки такі коливання високочастотні, то вони, не зважаючи на їх малу потужність, можуть розповсюджуватися на сотні метрів. А у зв'язку з тим, що для будь-якої апаратури наявними є нелінійні елементи (транзистори та транзисторні мікросхеми), то на них відбувається модуляція інформаційними сигналами, яка формується у вигляді сигналу паразитного випромінювання. Окрім того, що ці сигнали можуть бути перехопленими з ефіру, вони ще й гарантують утворення наводок.

Наводка – це сигнал, який утворюється у будь-якій струмопровідній конструкції (наприклад, на трубах центрального опалення) через явище самоіндукції. Тобто, змінне електромагнітне поле (електромагнітна хвиля), попадаючи на будь-який нерухомий провідник, викликає в останньому появу змінного струму. А оскільки паразитне випромінювання несе на собі небезпечні сигнали, то їх можна зняти з будь-яких струмопровідних конструкцій та мереж.

9.4 Організаційно-технічні заходи щодо ТЗІ на об'єкті

Система захисту об'єктів від витоку інформації складається із організаційних та технічних заходів, метою яких є ліквідація або суттєве зменшення можливості витоку конфіденційної інформації, а також контролю захищеності технічних засобів під час їх експлуатації.

Організаційний захід – це захід із захисту інформації, проведення якого не потребує застосування спеціально розроблених технічних засобів.

До основних організаційних і режимних заходів відносяться:

– проведення робіт із захисту інформації організаціями, які мають ліцензію на діяльність у сфері захисту інформації;

– категоріювання та атестація об'єктів ТЗПІ та виділених для проведення закритих заходів приміщень по виконанню вимог забезпечення захисту інформації при проведенні робіт із відомостями відповідного ступеню таємності;

– використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

– встановлення контрольованої зони біля об'єкта;

– залучення до робіт з будівництва, реконструкції об'єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в сфері захисту інформації за відповідними положеннями;

– організація контролю й обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

– введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, які підлягають захисту;

– відключення, на період закритих заходів, технічних засобів, які мають елементи, які виконують роль електроакустичних перетворювачів (лінії зв'язку тощо).

Технічний захід – це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень. Технічні заходи включають у себе:

– встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

– перевірку техніки, яка використовується, на відповідність величини паразитних випромінювань допустимим рівням;

– екранування приміщень або техніки, яка використовується;

– перемонтаж окремих мереж, кабелів та ліній зв'язку;

– застосування спеціальних пристроїв і засобів захисту;

– використання засобів активного захисту;

– перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз.

На початку робіт із ТЗІ необхідно визначити види інформації й від якого роду загроз необхідно її захищати. Для цього в першу чергу визначають категорію приміщення. При цьому з'ясовують види та ступень таємності

інформації, що може циркулювати у приміщенні. Далі розглядають конструктивні особливості приміщення та умови його розташування, наявність побутової техніки та апаратури для обробки інформації, її типи та технічні характеристики. З'ясовується та враховується наявність навколо об'єкту, який необхідно захищати, іноземних установ, автостоянок, приватних фірм (тобто місць, з яких можливо організувати стаціонарне та мобільне зняття інформації). Заміряється відстань до таких місць і визначається охоронна зона, в межах якої несанкціоноване зняття інформації вважається неможливим. Це надає змогу з'ясувати типи та ступень можливих загроз й встановити відповідну категорію захисту інформації.

Якщо поряд із об'єктом є іноземні установи чи фірми, де можна організувати стаціонарне зняття інформації, категорійність приміщення підвищується на один ступінь. Складається акт про встановлення категорійності приміщення, в якому відбиваються всі питання, що перераховані вище.

Встановлення категорійності приміщення надає змогу скласти план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об'єкті. Ці роботи повинен проводити ліцензіант, тобто установа, яка має державну ліцензію на проведення таких робіт. Надалі усі роботи із ТЗІ проводяться лише ліцензіантом.

Якщо в установі є підрозділ з ТЗІ, який має ліцензію на виконання усього необхідного обсягу робіт, то ці роботи можуть проводитися таким підрозділом.

При проведенні робіт із ТЗІ необхідно провести ряд заходів, зокрема:

– визначити та змонтувати необхідні технічні засоби, які необхідні для захисту інформації на об'єкті;

– провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Після проведення усього комплексу технічних робіт ліцензіант разом із замовником складають акт про надання об'єкту певної категорії із захисту інформації. Лише після одержання та затвердження такого акту на об'єкті можна обробляти інформацію з обмеженим доступом.

Технічний захист інформації від її несанкціонованого зняття полягає у застосуванні спеціальних технічних методів захисту, які блокують потенційні канали витоку інформації, тобто заважають спробам її незаконного отримання.

Для того, щоб захищати інформацію від витоку необхідно володіти інформацією про потенційні канали витоку та методи їх блокування. Під час

вивчення методів та засобів технічного захисту інформації перевагу надають класифікації каналів витоку та методів несанкціонованого зняття інформації. Такий порядок надання матеріалу пояснюється тим, що для того, щоб захищатися від якоїсь загрози, необхідно знати, що вона собою являє. При цьому значна увага приділяється сучасним способам беззаходного (дистанційного) зняття інформації, зокрема, способам високочастотного нав'язування.

9.5 Основи несанкціонованого зняття інформації способом та засобами високочастотного нав'язування

Вперше зняття акустичної інформації способом високочастотного нав'язування (ВЧН) було здійснено у 1945 р., коли делегація піонерів подарувала американському послу в СРСР зроблений власноруч гіпсовий герб США, а розчулений посол повісив його у власному робочому кабінеті над своїм столом.

У «подарунку» було вмонтовано пасивний акустичний резонатор, який опромінювався зовнішнім радіосигналом стабільної частоти, яка відповідала власній резонансній частоті резонатора.

Під дією акустичних хвиль, які виникали під час розмов у кабінеті, резонансна частота резонатора змінювалася. Відповідно відбитий радіосигнал ставав модульованим сигналом розмов, які велися у кабінеті.

Таким чином до 1951 р., коли спецслужби США нарешті виявили цю пасивну радіозакладку, керівництво СРСР володіло про зміст усіх розмов, які велися в кабінеті посла США.

Цей спосіб зняття інформації отримав назву високочастотне нав'язування.

В подальшому цей спосіб набув свого подальшого розвитку, а спеціалісти зрозуміли, що він може використовуватися і для зняття інформації з будь-якого елемента, який має власну резонансну частоту.

Для того, щоб з'ясувати принцип ВЧН, необхідно розглянути явище резонансу у резонансному контурі.

На рисунку 9.6 подано паралельний резонансний контур. Він складається із котушки індуктивністю L, конденсатора ємністю C та резистора опором R. Індуктивний опір котушки рівний:

$$R_L=jL\omega,$$

ємнісний опір конденсатора:

$$R_C=1/(jC\omega),$$

а кругова частота:

$$\omega=2\pi f,$$

де L – індуктивність котушки;

C – ємність конденсатора;

f – частота гармонійного сигналу, який подається на котушку та конденсатор;

$j = \sqrt{-1}$.

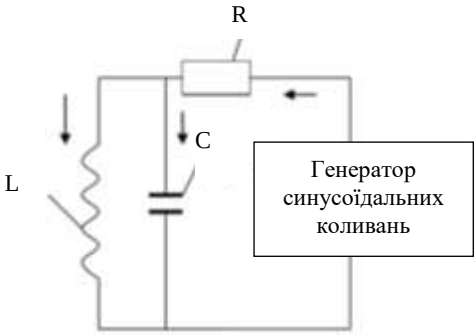

Рисунок 9.6 – Паралельний резонансний контур

З рисунка 9.6 видно, що максимальний рівень напруги сигналу на котушці та конденсаторі у місці їх з'єднання з резистором буде тоді, коли струм у котушці та конденсаторі буде однаковим за своєю силою. Це й є умовою резонансу. Тобто, опір котушки та конденсатора на частоті резонансу рівні. Отже:

$$jL\omega = \frac{1}{jC\omega},$$

звідки резонансна частота буде рівною:

$$f = \frac{1}{2\pi\sqrt{LC}}.$$

Розглянемо частотну характеристику резонансного контуру (тобто залежність рівня напруги у точці з'єднання елементів L, C і R відносно частоти, яка подається від генератора синусоїдальних коливань змінної частоти). Зі зростанням частоти опір котушки зростає, а опір конденсатора падає. Тому, зліва від резонансу струм у контурі має індуктивний характер, справа – ємнісний, що й показано на рисунку 9.7.

При ВЧН на резонансний контур ззовні подають синусоїдальний сигнал резонансної частоти. Тиск акустичної хвилі змінює резонансну частоту контуру. При цьому резонансна крива і точка резонансу зміщується вліво або вправо відносно точки власної резонансної частоти, яка була без дії акустичного

сигналу. Частота зовнішнього сигналу при цьому не змінюється, отже він припадає на ліву або праву частину резонансної кривої, а відбитий сигнал стає модульованим мовним сигналом.

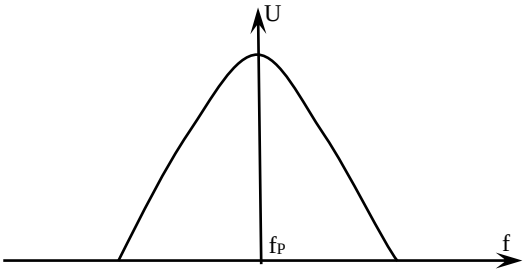

Рисунок 9.7 – Резонансна крива

9.6 Класифікація каналів витоку інформації

Як зазначалось вище під технічним каналом витоку інформації слід розуміти сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого збирається інформація про об'єкт, і фізичного середовища, де розповсюджується інформаційний сигнал.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР більш детально технічні канали витоку інформації можна поділити на:

– радіоканали (електромагнітне випромінювання радіодіапазону);

– електричні (засоби провідникового зв'язку та різні струмопровідні комунікації);

– акустичні (розповсюдження звукових коливань);

– оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектру).

На рисунку 9.8 приведено загальну характеристику каналів витоку оптичної, акустичної, електронної та електромагнітної інформації. Деякі з цих каналів можуть бути комбінованими, тобто бути каналами витоку для декількох видів інформації.

Так, скляні конструкції та вікна можуть бути каналами витоку для акустичної та оптичної інформації, але через них можна зняти також електронну й друковану інформацію (зокрема, текст з екрану ПЕОМ). З телефонного апарату можна зняти акустичну інформацію, а також електронну та електромагнітну тощо.

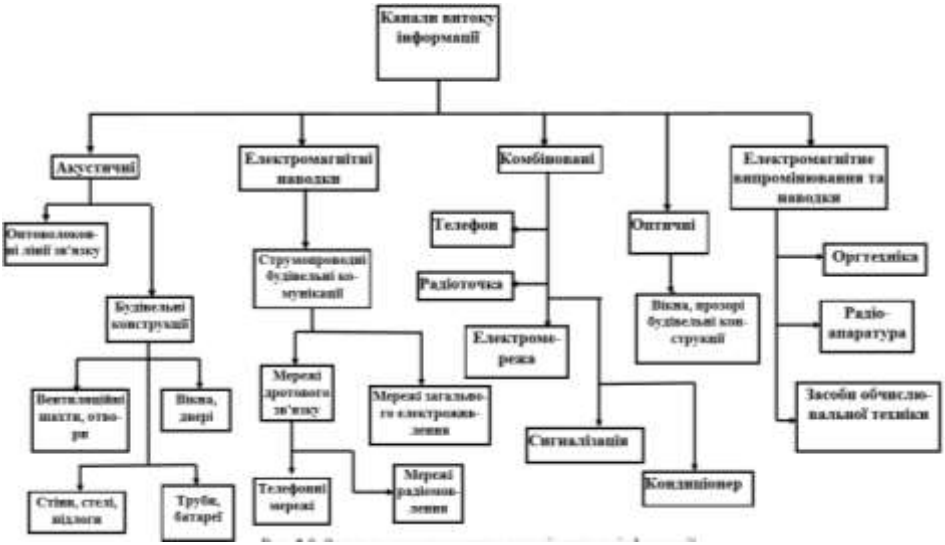

Рисунок 9.8 – Загальна характеристика каналів витоку інформації

Отже, для розуміння принципів технічного захисту інформації необхідно знати способи і засоби її зняття, оцінити реальність загроз використання для цього різних каналів.

Способи та засоби зняття акустичної інформації, які використовуються на сьогодні, наведено на рисунках 9.8-9.11.

На рисунку 9.9 наведено практично усі відомі методи та засоби комбінованого зняття акустичної інформації: спочатку вказано канал витоку, а потім можливі способи та засоби зняття інформації. Відповідно до розташування та облаштування об'єкту, що охороняється, можливо використання різних каналів витоку. При цьому можуть використовуватися різні види перетворення та способи і засоби перенесення інформації. Наприклад, акустичну інформацію можна зняти в приміщенні за допомогою радіомікрофону, який живиться від струму електромережі, а можна виконати цю операцію за допомогою дротового мікрофону, який також підключено до електромережі. В цьому випадку інформація буде передаватися електромережею і її можна зняти навіть на трансформаторній підстанції.

Для зняття акустичної інформації із закритого приміщення дедалі частіше використовується ВЧН, коли для зняття інформації використовується будь-який «цінний» подарунок, виконаний так, щоб він став резонансним елементом модуляційної системи. При ВЧ випромінюванні цього елементу відбувається

модуляція мовними сигналами спрямованого на цей елемент високочастотного радіовипромінювання. Таким самим чином, розрахувавши або експериментально з'ясувавши резонансні характеристики резонансного кола телефонного апарату чи, наприклад, трансформаторного кола радіоточки, можна зняти мовну інформацію за допомогою високочастотного нав'язування.

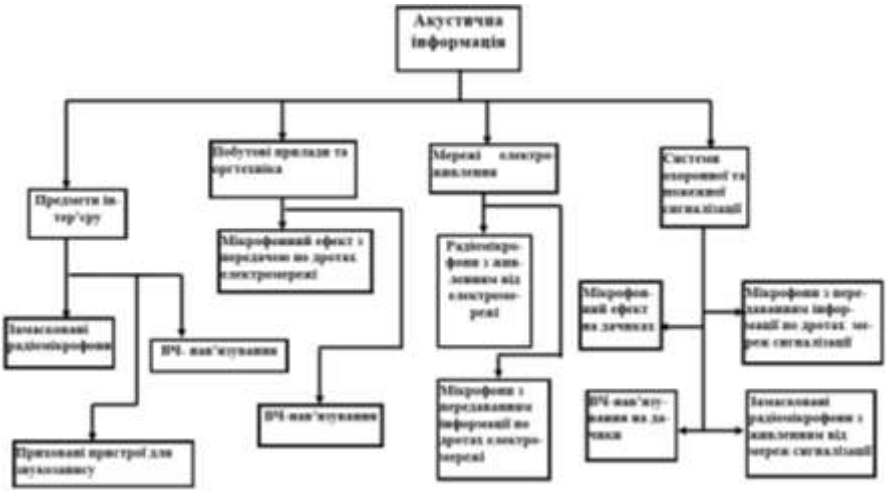

Рисунок 9.9 – Комбіновані методи та засоби зняття акустичної інформації

В закритих приміщеннях (рис. 9.10) акустичну інформацію можна знімати за рахунок того, що будівельні конструкції (стіни, підлоги, стелі, вікна, труби, зачинені двері) є по суті акустичними мембранами та чудово передають звукові коливання. Таким чином, за допомогою віброперетворювача та підсилювача можна знімати акустичний сигнал з будь-якого приміщення через стіну, підлогу або стелю. На відстані акустичний сигнал можна зняти з зачинених вікон, спрямувавши випромінювання лазеру на скло чи скористувавшись спрямованим мікрофоном.

Акустичну інформацію можна знімати також з побутових приладів та апаратури зв'язку (рис. 9.11).

Особливо небезпечним приладом є телефон. Наявність незахищеного телефонного апарату в режимному приміщенні дає змогу без зайвого клопоту прослухувати в ньому всю акустичну інформацію навіть не використовуючи радіомікрофони або іншу дорогу спецтехніку. При чому це можна робити навіть тоді, коли трубка лежить на апараті, тобто телефон, здається, виключено. Але до складу електричного кола телефону входять елементи, які здатні створити

резонансний контур, який постійно підключено до телефонної мережі напругою від 40 до 60 В. Частина з них ще й мають властивості мембрани, яка коливається під дією акустичного сигналу, тобто механічних коливань повітря.

Рисунок 9.10 – Методи та засоби зняття акустичної інформації із будівельних конструкцій

Рисунок 9.11 – Методи та засоби зняття акустичної інформації із засобів та ліній зв’язку

Під час коливань такої мембрани відбувається зміна резонансних характеристик контуру (мікрофонний ефект). При розмові, у разі наявності такого «шпигуна», на резонансному контурі відбувається модуляційний процес звуковими коливаннями мови, тобто акустичний сигнал перетворюється в електричний. Цей сигнал надходить до дротів телефонної мережі, звідки його можна зняти за допомогою простого пристрою. Не говорячи уже про застосування ВЧН або зняття сигналів за допомогою індукційного давача, чи давача із високим вхідним опором, які можна підключити до лінії зв'язку за межами приміщення або, навіть, до об'єктів, які взагалі надзвичайно важко виявити (практично неможливо без застосування спеціальних приладів, що вимірюють неоднорідність мережі).

Мають свої резонансні контури та мембранні елементи інші побутові прилади: кондиціонери, оргтехніка. В цьому випадку акустичну інформацію можна зняти з електричної мережі, до якої вони підключені.

Насамкінець, завжди існує загроза встановлення радіомікрофону (інколи його називають радіозакладним пристроєм або радіозакладкою чи «жучком»).

На рисунку 9.12 наведено сучасні варіанти виконання цих дуже шкідливих пристроїв – від найпростішого та найдешевшого, які, всупереч законодавству, сьогодні можна придбати, до найскладнішого (з шумоподібною несучою частотою), який є майже «невидимкою» для сучасних приладів контролю за ефіром.

На щастя, такі закладки дуже дорого коштують та виготовляються на спеціалізованих виробництвах лише для правоохоронних органів. Але не виключено, що подібними приладами можуть бути оснащені злочинні угруповання та служби безпеки окремих фінансово-промислових груп.

З огляду способів та засобів зняття акустичної інформації видно, як багато загроз для викрадення цього виду інформації надає сучасна техніка. Але, нажаль, окрім акустичної інформації, сучасна техніка перехоплення надає можливості знімати електронну чи електромагнітну інформацію, тобто фактично викрадати будь-які документи, які створюються, передаються та зберігаються у незахищених засобах електронної обробки інформації.

Канали витоку інформації (рис. 9.8) дають наочне уявлення про такі можливості. Додамо, що для їх реалізації застосовуються усі найсучасніші математичні теорії, технічні засоби та способи. В першу чергу використовуються методи та засоби спектральної обробки сигналів, які, хоч і базуються на винайденій ще у XVIII столітті математичній теорії рядів Фур'є, але знайшли свій науковий розвиток і технічне застосування та реалізацію лише

у XX століття. Нині ці методи отримали широке визнання та розвиток. Цей розвиток складається як із розробки нових засобів (пов'язано із розвитком технологій створення та виробництва нових виробів мікроелектроніки), так і розвитком прикладної математики, яка надає нові алгоритми обробки інформації та нові, більш точні та продуктивні, методи перетворення сигналів (вейвлет-перетворення).

Рисунок 9.12 – Види радіомікрофонів (радіозакладних пристроїв) для зняття акустичної інформації

Слід відзначити, що усі методи мають універсальний характер, тобто вони можуть застосовуватися у медицині, військовій справі, керуванні технологічними процесами та у багатьох інших галузях життя та народного господарства. Ці методи використовуються не лише для перехоплення, але й для захисту інформації.

Спочатку розглянемо методи зняття інформації, які подаються в електронному вигляді. Канали витоку такої інформації можуть бути спільними з каналами витоку акустичної інформації (рис. 9.8). Знімання інформації, яка представлена в електронному вигляді, проводиться за рахунок того, що усі електронні прилади (в тому числі – обчислювальна техніка та оргтехніка) мають паразитне електромагнітне випромінювання на високих частотах. Уникнути цього явища принципово неможливо, бо воно пов'язане із конструктивно-технологічними особливостями радіокомпонентів, з яких виготовляють будь-яку електронну техніку. Паразитне випромінювання за рахунок нелінійності амплітудних характеристик, яка також завжди присутня в електронному обладнанні, модулюється сигналами інформації, які оброблюються, та у вигляді модульованих інформацією коливань випромінюється в ефір.

Крім того, такі коливання, зважаючи на їх високочастотний характер, потрапляють через ланцюги вторинного електроживлення до електромережі. Також, у вигляді електромагнітних наводок, вони потрапляють на усі струмопровідні частини приміщення, де розміщено електронну апаратуру.

Зрозуміло, що рівень цих паразитних коливань малий. Взагалі він не перевищує рівня власних шумів апаратури, який завжди роблять як можна меншим, щоб розширити динамічний діапазон апаратури. Але навіть цього вкрай малого рівня паразитних сигналів вистачає для перехоплення інформації за допомогою сучасної чутливої апаратури для її несанкціонованого зняття.

Таку апаратуру може бути розміщено, наприклад, в легковому автомобілі, який поставлено на стоянку поряд з об'єктом. Перехоплення інформації із незахищених комп'ютерів нестаціонарними засобами може провадитись з відстані 200…300 м. При перехопленні за допомогою стаціонарних потужних засобів, які розміщаються, як правило, у дипломатичних представництвах або інших стаціонарних об'єктах розвідки та контррозвідки, перехопленням може бути охоплено великий регіон.

Для глобального зняття інформації з розвідувальними цілями використовуються супутники Землі та стаціонарні пункти розвідки.

На рисунку 9.13 подано канали та засоби зняття електромагнітної інформації. З нього видно, що інформацію в електронному та електромагнітному вигляді можна знімати з ліній зв'язку та з електронної апаратури, яка призначена для обробки інформації.

Для перехоплення інформації з ефіру використовують так звані панорамні радіоприймачі (під час роботи на стаціонарному розвідувальному об'єкті) та малогабаритні сканери (для роботи на пересувному об'єкті). Ці прилади мають

багато різних функцій та здатні приймати сигнали з різними видами модуляції, слідкувати за частотою станції, працювати під керуванням комп'ютера та т. інше.

Рисунок 9.13 – Канали та засоби зняття електромагнітної та електронної інформації

Для зняття інформації з ліній зв'язку шляхом підключення використовуються давачі з високим вхідним опором для паралельного вмикання або індукційні давачі для безконтактного перехоплення сигналів. Визначити їх наявність на лінії зв'язку без складних спеціалізованих пристроїв практично неможливо.

Для зняття інформації, яка наводиться на струмопровідні конструкції приміщення використовуються спеціальні приймачі наводки, які побудовано за принципом частотно-селективного підсилювача з великим коефіцієнтом підсилення та, відповідно, значним динамічним діапазоном. При обробці отриманої, таким чином, інформації для підвищення співвідношення

сигнал/завада використовують апаратуру спектральної обробки сигналів. Так само відбувається зняття інформації, яка надходить до електромережі у вигляді модульованого сигналу паразитного випромінювання або ж у вигляді наводки.

Письмова інформація може бути отримана у двох видах: як оптична і як електронна. Електронна інформація може бути отримана шляхом зняття з ліній зв'язку (факсимільний зв'язок чи електронна пошта), або перехоплення каналів паразитних випромінювань та наводок (наприклад, дисплей комп'ютера, який, до речі, має найбільший рівень паразитного випромінювання).

В електронному вигляді письмову інформацію можна отримати також шляхом копіювання магнітних або оптичних носіїв, копіюванням шляхом зняття із паперового документа електронної копії на сканері.

Оптична інформація може бути отримана шляхом використання прихованих телекамер, які можуть працювати або у інфрачервоному, або у діапазоні видимих хвиль. Окрім того, можуть бути використані фотоапарати, копіювання шляхом зняття ксерокопій і звичайної крадіжки.

Шляхи отримання письмової інформації наведено на рисунку 9.14.

Рисунок 9.14 – Шляхи отримання письмової інформації

Для зняття оптичної інформації зазвичай використовують оптичні та електронно-оптичні пристрої. Серед оптичних пристроїв слід відзначити біноклі, фотоапарати, підзорні труби, кінокамери, тобто засоби прямого оптичного спостереження та фіксації оптичної інформації без застосування електронних приладів. Серед оптично-електронних приладів слід відзначити відео- та

телекамери, цифрові фотоапарати, прилади нічного бачення, інфрачервоні приціли, лазерні прилади спостереження та лазерні приціли.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Складові ІБ, які відносяться до технічного аспекту інформаційної безпеки
2. Технічний та криптографічний захист інформації.
3. Технічний каналу витоку інформації.
4. Небезпечний фізичний сигнал.
5. Класифікація технічних каналів витоку інформації.
6. Природні та штучні ТКВІ.
7. Загальна класифікація видів інформації.
8. Схема обробки, розповсюдження та захисту інформації.
9. Додаткові технічні засоби і системи.
10. Фізична сутність акустичного сигналу.
11. Фізична сутність акустично-електричних перетворень.
12. Фізична сутність мікрофонного ефекту.
13. Фізична сутність процесу модуляції та демодуляції.
14. Механізм утворення наводок? Де вони виникають? 31. В чому полягає небезпека паразитних випромінювань та наводок.
15. Організаційні та технічні заходи захисту об’єкту.
16. Канали витоку акустичної, електромагнітної та електронної інформації інформації.

Література: [2; 5-11; 14-17].

Тема 10. Методи та засоби блокування технічних каналів витоку інформації

План:

10.1 Загальні положення технічного захисту інформації

10.2 Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації

10.3 Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв

10.4 Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами

10.5 Захист інформації від несанкціонованого запису звукозаписувальними пристроями

10.6 Захист електронної інформації
10.7 Захист письмової інформації від оптичного зняття

10.1 Загальні положення технічного захисту інформації

Об'єктом технічного захисту інформації є будівля, приміщення, окремий основний технічний засіб або їх група, яка об'єднана загальним призначенням та підлягає захисту від технічних розвідок.

Як видно з визначення, об'єкт може бути як однією із складових, так і може об'єднувати у собі усі згадані складові. Все залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, у яких приміщеннях об'єкту циркулює ця інформація. Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень. Якщо треба захищати велику кількість приміщень (велику група, яка, наприклад, складається з підгруп), об'єкт захисту може складатися із усієї будівлі. Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об'єкту, то використовується комплексний захист інформації. При цьому і сам об'єкт захисту може розміщуватися всередині іншого об'єкту, який не є в цілому об'єктом захисту інформації.

Основні технічні засоби – це технічні засоби, призначені для обробки, зберігання та передавання закритої інформації.

Існують й допоміжні технічні засоби та системи, які призначені для обробки відкритої інформації. Але вони можуть утворювати технічні канали витоку закритої інформації. Отже, переходячи до захисту інформації на певному об'єкті, необхідно, в першу чергу, визначити, які види інформації підлягають захисту, а, по-друге, які приміщення у будівлі (або всю будівлю) необхідно захищати. Також необхідно знати ступень таємності інформації, що підлягає захисту.

Окрім цього, необхідно обов'язково володіти інформацією про загрози для інформації, які можуть виходити від потенційного супротивника. Загроза для інформації – це витік, можливість блокування або порушення цілісності інформації, яка може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації. Варто пам'ятати, що володіння інформацією про у ці складові, дозволить розробити систему захисту інформації на об'єкті.

При цьому слід пам'ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування,

отже треба користуватися тими системами та засобами захисту, які найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об'єкті.

У випадку комплексного захисту необхідно розробляти підсистеми захисту для кожного окремого виду інформації, обов'язково пов'язавши їх у комплексну систему. При цьому необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з рівнем технічного захисту, відповідним ступеню таємності інформації та рівню потенційних загроз.

Рівень технічного захисту інформації – це сукупність вимог, в тому числі й тих, які нормуються, які визначаються режимом доступу до інформації та загрозами для її безпеки. У технічному захисті інформації прийнято розрізняти два основні методи захисту: пасивний та активний.

Активний захист побудовано на постановці перешкод зняттю інформації шляхом випромінювання завад у канал витоку, рівень яких перевищує рівень небезпечних сигналів, які можна із них зняти. До активного захисту також відносять методи протидії, які засновано на постійному контролі середовища розповсюдження небезпечних сигналів необхідними для цього приладами та комплексами, які дозволяють виявляти спроби зняття інформації та активного пошуку і знешкодження засобів зняття інформації.

Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, наприклад, шляхом екранування електромагнітного випромінювання.

Для технічного захисту інформації притаманним є використання обох напрямків захисту. При цьому, слід відзначити, що пасивні методи захисту не використовують фізичних процесів, які є шкідливими для здоров'я оточуючих та заважають повсякденній діяльності людей. Однак у більшості випадків застосування активних методів захисту є необхідним, які разом із пасивними методами захисту забезпечують необхідний ступінь рівня технічного захисту інформації.

10.2 Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації

Першочерговим завданням під час розроблення проекту та обладнання об'єкту для його захисту від витоку інформації є встановлення технічних каналів витоку інформації для кожного конкретного приміщення.

Зокрема, серед акустичних каналів витоку можуть бути й такі, які зумовлені

конструктивними особливостями приміщення, так і ті, що створені навмисно (особливий інтерес приділяють старим спорудам та блочним бетонним спорудам, у яких звуководні канали формуються на стиках блоків).

Для проведення робіт із захисту акустичної інформації використовують прилади для загальних акустичних вимірювань та спеціалізована апаратура, яка побудована на тих самих принципах, що й апаратура для зняття інформації. Окрім цього, органолептичній перевірці піддаються усі приміщення, які можуть бути пов'язані із об'єктом захисту створеними навмисно звуководними каналами. При цьому, як правило, користуються повними будівельними планами усієї будівлі, де розміщено об'єкт захисту. Одночасно перевіряють відсутність (чи наявність) засобів зняття інформації на виявлених каналах витоку. Під час проведенні таких робіт особливу увагу приділяють можливості несанкціонованого зняття акустичної інформації з металевих трубопроводів (опалення, вентиляція та водопостачання).

Після проведення обстеження на базі отриманих результатів вимірювань та розрахунків складають паспорт об'єкту та проектують систему його захисту (обирають типи та кількість необхідної апаратури, місця розташування випромінювачів тощо).

Захиститися від витоку акустичної інформації через зачинені вікна та через стіни, стелю й підлогу можна шляхом використання спеціальних генераторів випадкових або псевдовипадкових електричних коливань, які навантажено на перетворювачах електричного сигналу в механічні коливання. Такі генератори створюють маскуючий механічний сигнал, який заважає приймати мовні сигнали на перетворювачі, які застосовуються у ході зняття акустичної інформації.

Зазвичай, перетворювачі генераторів розміщують на склі та стінах, підлозі й стелі. Зрозуміло, що спочатку необхідно з'ясувати можливість такого зняття інформації із суміжних приміщень (тобто можливість проникнення в суміжні приміщення сторонніх осіб). Захищати вікна в приміщеннях, де циркулює інформація з обмеженим доступом, необхідно в тих випадках, коли вони виходять на незахищений простір, якщо охоронна зона (відстань від вікна до периметру охорони) не перевищує 200 м. Такий захист ефективно діє також проти зняття акустичної інформації з вікон за допомогою лазерного випромінювання та спрямованого мікрофону.

Генератори вібрацій можна віднести до активних методів захисту, бо ці вібрації є активною завадою для акустичних сигналів та діє на середовища, з поверхні яких їх намагаються зняти. Також до активних методів захисту як від

прослуховування через будівельні конструкції мембранного типу, так і від прослуховування за допомогою різних типів мікрофонів, можна віднести генератори акустичного шуму, який випромінюється у повітря приміщення, що захищається. Зрозуміло, що при роботі таких генераторів вести розмову дуже неприємно, бо шум, що випромінюється, заважає розмовляти.

На сьогодні відомо про комбіновані генератори, які побудовано на принципі: завада не повинна заважати тому, хто її використовує. Існує три загальні тенденції розробки таких генераторів.

Перша тенденція – використання зворотного зв'язку для регулювання спектру шумового сигналу та його рівня залежно від рівня акустичного сигналу, який треба маскувати.

Друга тенденція – створення закритого ланцюга зв'язку для розмов між учасниками переговорів. Вона реалізується або за рахунок шифрування розмов, що передаються в ізольованому від навколишнього акустичного середовища колі, або шляхом використання поза ним спеціальної завади, яка не дозволяє зняття розбірливої акустичної інформації за межами цього кола.

Третя тенденція – використання змішаної завади, яка складається із тихої музики, шуму та голосових сигналів декількох учасників розмови, які зсунуті у часі та інвертовані за спектром. Така суміш сигналів не дозволяє зняти розбірливі сигнали розмови. Навіть якщо записати розмову, яка замаскована таким чином, та очистити її відомими нині методами, неможливо отримати розбірливих сигналів. При цьому методі маскування рівень завад, які випромінюються у приміщенні, значно нижчий від рівня шуму, який випромінюється при застосуванні звичайного генератору. Такий шум не заважає розмові та не є шкідливим для здоров'я оточуючих.

Захист від будь-яких (радіо- чи звичайних, з провідниковим зв'язком) мікрофонів, що встановлено у приміщенні, може бути виконаний також методом «завантаження» його мембрани. При застосуванні цього методу у повітря випромінюється акустична завада у вигляді модульованих ультразвукових сигналів високого рівня, які діють на мембрану мікрофону з таким тиском, що інші акустичні коливання меншого рівня мікрофонами не сприймаються. До недоліків цього методу захисту слід віднести шкідливий вплив на людину та зовнішнє середовище ультразвукових коливань високого рівня та дуже швидке затухання таких коливань у повітрі.

На практиці відомо про ще один метод захисту акустичної інформації, який пов'язаний із встановленням електромагнітної завади від генераторів радіочастотного випромінювання. Він дозволяє нав'язати шумову або, навіть,

будь-яку іншу акустичну інформацію на нелінійні елементи апаратури звукозапису та з'єднуючі провідники мікрофонів. Цей метод засновано на випромінюванні у навколишнє середовище широкосмугової модульованої радіохвилі з енергією, яка є достатньою для наведення на елементи апаратури зняття інформації сигналів завади, що повністю блокують її функціонування.

На сьогодні генератори вібраційних та шумових коливань, які призначено для захисту інформації, яка обговорюється в службових приміщеннях, методом вібраційного та акустичного зашумлення, прийнято монтувати на поверхнях конструкцій, які огороджують приміщення, та у відкритому просторі завад із рівнями, які виключають можливість виділення конфіденційної інформації з суміші сигналу з завадою. Такі генератори володіють 4-ма каналами формування завад, до кожного із яких підключається від 30 до 40 вібраторів п'єзоелектричного типу, до 10 вібраторів електромагнітного типу або акустичних систем, які забезпечують перетворення в конструкціях, які відгороджують приміщення, електричного сигналу в механічні коливання або в акустичні коливання. Разом із створенням традиційної шумової завади для підвищення ступеню маскування мовної інформації генератор може формувати нестаціонарну заваду у вигляді суміші трьох сигналів від станцій радіомовлення, для чого є три вбудовані радіоприймачі. В ході роботи здійснюється автоматичне перестроювання робочої частоти кожного з приймачів. Перестроювання робочої частоти здійснюється за випадковим законом як у часі, так і по радіостанціях за рядом встановлених заздалегідь частот. Для корекції амплітудно-частотної характеристики (АЧХ) приміщення кожний з каналів має вбудований еквалайзер (корегувач частотної характеристики під акустичні особливості приміщення) на п'ять смуг.

Для захисту від витоку інформації з приміщення, де розташовано телефонний апарат, використовуються прилади, які забезпечують блокування зняття інформації при покладеній трубці за рахунок мікрофонного ефекту дзвінкового ланцюга. Залежно від типу АТС, до якої підключено телефон, використовуються різні моделі приладів: для аналогової або квазіелектронної АТС; для цифрової АТС.

Прилади першої групи вмикаються у розрив ланцюга між телефонним апаратом та телефонною розеткою на кожний провідник мережі. В основу їх роботи покладено нелінійність характеристики напівпровідникових діодів, що надає змогу не перепускати через прилад електричні сигнали малої амплітуди до 0,4 В, які виникають у дзвінковому ланцюзі за рахунок мікрофонного ефекту.

Фільтр низьких частот дозволяє захистити телефон від зняття інформації методом ВЧ-нав'язування на дзвінковий ланцюг.

Прилад другої групи будуються за принципами першої, але із врахуванням особливостей цифрових АТС. Ці прилади дозволяють ефективно захистити акустичну інформацію в приміщенні від витоку телефонними каналами при покладеній трубці.

Значно складніше захистити інформацію від зняття під час розмови по телефону. Існує декілька видів приладів, які спроможні визначати підключення до телефонної мережі приладів, що живляться від цієї мережі. Це найпростіші прилади виявлення підслуховуючи пристроїв та несанкціонованого підключення до телефонної мережі, таких приладів багато. Хоча вони і відрізняються один від одного, але використовують однакові принципи, тобто реагують на падіння напруги у мережі (дуже незначні), які виникають при підключенні додаткових споживачів електричного струму. Більш складні прилади такого типу можуть «пригнічувати» виявлені підслуховуючі пристрої, блокувати несанкціоновані паралельні телефони тощо (зазвичай такі пристрої потребують окремого підключення до мережі 220 В, мають додаткові регулятори та індикатори).

Однак, слід враховувати, що усі такі прилади можуть контролювати телефонну мережу лише від апарату до АТС. Підключення на АТС можливо лише у одному випадку – з відповідного дозволу суду технічними службами правоохоронних органів. Але у цьому випадку підключення не може бути виявлено жодним приладом.

Саме тому, необхідністю, на сьогодні, є такі прилади, які надійно б виявляли «інтелігентні» способи зняття інформації з телефонних ліній (наприклад, способом індукційного зняття або пристроями з надвисокими вхідними опорами та відповідно малими ємностями). Варто зазначити, що такий прилад існує, а його робота базується на принципі рефлектометра та визначає неоднорідності лінії (локаторрефлектометр).

Такий прилад здатний витримувати напругу сигналу виклику АТС (до 150 В) та забезпечує перевірку та визначення місця неоднорідності у лінії на відстані до 400 м. Можливість виявлення засобів зняття інформації за допомогою локатораре флектометра не менше 95%, тоді як всі інші нічого не гарантують щодо можливостей виявлення. Під час роботи цих приладів не потрібно відключати лінії від АТС. Вихід приладу вмикається в телефонну розетку замість телефонного апарата. При надходженні виклику на даний номер, під час роботи локатора, відбувається його автоматичне відключення на момент проходження сигналу виклику. Результати виявлення видаються на цифровий

індикатор у метрах, послідовно від кожного наступного об'єкта. Також видається номер об'єкта.

Деякі «фахівці» вважають, що для рефлектометра характерна «...низька достовірність отриманих результатів вимірювання (найчастіше за неоднорідність приймають контактні з'єднання)...». Але саме цей недолік і його перевагою. Висока чутливість рефлектометрії дозволяє виявляти ємнісне підключенні від 25 пФ, індуктивне – від 10 мкГн. Визначення іншими засобами подібної зміни параметрів лінії є достатньо проблематичним. Більш того, вказується дальність до місця зміни параметра, що є необхідним під час пошуку.

Простота в обслуговуванні дозволяє дуже швидко провести паспортизацію лінії із одночасним виявленням і знищенням всіх, вже наявних засобів зняття інформації. Після паспортизації лінії прилад дозволяє швидко здійснювати контроль, виявлення і ліквідацію об'єктів, які з'явилися та не відповідають паспорту лінії.

На сьогодні, з точки зору, не вразливості виявлення залишається один клас засобів несанкціонованого зняття інформації – засоби знімання інформації із безконтактним вмиканням у лінію – індуктивні датчики та датчики типу «телефонне вухо». Це викликано тим, що ці пристрої не вносять змін у динамічні параметри лінії, а внесена ними неоднорідність настільки незначна, що рефлектометр може виявити її тільки при зондуванні надкоротким імпульсом, але при цьому різко обмежується дальність його дії.

Так, при тривалості імпульсу, що зондує, 500 пс максимальна дальність виявлення з можливістю 90% складатиме не більш ніж 20…25 м.

Варто пам'ятати, що жодні прилади, які використовуються з одного боку лінії, не можуть виявити наявність засобів зняття інформації на протилежному кінці зв'язку, тобто у абонента, з яким ведеться розмова (якщо він, звичайно, сам не потурбувався про захист своєї частини лінії). Тому для надійного захисту телефонних розмов слід використовувати «закриті» телефонні канали, де застосовується криптографічний захист інформації (скремблери).

Існує декілька принципів криптографічного захисту акустичної інформації. Відповідно до цього є й різні прилади захисту, які відрізняються різною вартістю та надійністю. Найбільш надійними є прилади та методи, які використовують вокодери та ліпідери з подальшим шифруванням. Принцип роботи таких пристроїв полягає у цифровій обробці аналогових сигналів, виявленні та розкладенні слів та звуків на окремі форманти та передачі мови у вигляді попередньо зашифрованому набору формант. При цьому ключове слово до шифру може мати довжину до 512 знаків, а інколи й ще більше (системи

надвисокої надійності). На розшифрування такої перехопленої розмови, як правило необхідно багато часу.

Існують і менш складні системи, які засновано на цифровій обробці спектру сигналів та передачі сигналів з іншим спектром. На приймальному кінці у відповідності із завданими правилами приймання відбувається зворотне перетворення сигналів.

Зрозуміло, що всі апарати криптографічного захисту інформації працюють у закритому режимі лише тоді, коли вони встановлені з обох кінців лінії зв'язку, тобто наявні у обох абонентів, що розмовляють між собою.

10.3 Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв

Оскільки радіозакладки мають мікрофон, то усі методи захисту від зняття за його допомогою діють також і на радіозакладні пристрої.

Всі наявні методи можна поділити на два підвиди, які здатні доповнити один одного. Перший, найбільш ефективний – це постійний радіомоніторинг ефіру. Метод полягає у постійній перевірці радіовипромінювань та виявленні нових складових у рисунку спектра (тобто, нових частот випромінювання), шляхом порівняння його із попереднім. При появі у контрольованій області спектру нових частотних складових проводять пошук передавача. Для цього використовують спеціальні прилади та методи пошуку, які складають сутність другого підвиду.

Але якщо перший підвид вимагає, в разі появи нових спектральних складових, застосувати інший, то останній може бути використаний автономно. Це метод періодичних оглядів, який застосовується на об'єктах, де відсутньою є апаратура для постійного контролю. Виконувати цю роботу повинні фахівці, які добре розуміються на радіотехнічних вимірюваннях та володіють методикою виявлення та знешкодження радіозакладок.

Розглянемо деяку апаратуру для радіомоніторингу ефіру та методи її застосування. Головним приладом, що входить до такої системи, є скануючий приймач (сканер). Такі приймачі мають вихід на персональний комп'ютер (другий елемент системи), з якого за допомогою спеціальної програми (третій елемент системи) провадиться керування режимами роботи сканера. Сканер може переналагоджуватись із заданим кроком дискретності за частотою. Окрім цього, він може працювати із сигналами, які мають різний вид модуляції та у різній смузі частот прослуховування (широкій та вузькій), має зменшувач шуму, індикацію режиму. Взагалі, сканер може працювати автономно від ПК, що й

використовується при пошуку радіозакладок.

На практиці існує і більш досконала апаратура, яка використовується у професійній радіорозвідці.

Програма моніторінгу побудована таким чином, що запам'ятовує спектр просканованої ділянки ефіру та використовує його як еталон під час порівняння із наступними вимірюваннями. Результати пошуку виводяться на монітор. У разі виявлення нових частотних складових у контрольованій зоні ПК видає сигнал тривоги. Система може працювати і в автоматичному режимі. На сьогодні багатьма фірмами розроблено такі програми, хоча і принцип їх побудови однаковий.

Робота комплексу з цією програмою побудована за принципом порівняння параметрів акустичних сигналів та працює таким чином:

1) На першому етапі вимірюється та запам'ятовується спектр радіосигналів за усім діапазоном роботи сканера. Одночасно встановлюється вид модуляції для кожного сигналу, випромінювання якого зафіксовано.

2) На другому етапі на кожній з виявлених частот комплекс випромінює у навколишнє середовище декілька складних акустичних сигналів, які сприймаються ним через ланцюг зворотного зв'язку, а саме – через радіоканал (приймач сканеру) на тій частоті, що перевіряється. Якщо в приміщенні є радіозакладка, то параметри сигналу, який продетектовано з ефіру, співпадуть з параметрами сигналу, що випромінювався у повітря приміщення. Для забезпечення однозначності сигналів, які сприймаються радіозакладкою, в сигнал, що випромінюється комплексом, додається акустичний сигнал з приміщення (шум, розмови та т. інше) через другий ланцюг зворотного зв'язку (мікрофон, підсилювач та змішувач сигналів).

Особливість комплексів, які побудовано на цьому методі, полягає у тому, що вони, по-перше, здатні виявляти наявність радіозакладних пристроїв з шумоподібною та випадковою несучою і, по-друге, локалізувати місце знаходження радіозакладок. Для цього у комплекси введено ряд додаткових пристроїв та програм. Такі комплекси використовуються для перевірки відповідності рівня захисту об'єкту технічним вимогам та надійності блокування каналів витоку акустичної інформації.

Окрім цього, під час використання додаткового конвертору наднизьких частот програма може виявляти пристрої підслуховування, які використовують кабельні комунікації для передавання звукової інформації із приміщення у діапазоні частот від 5 кГц до 2 МГц (мережа 220 В, кабель сигналізації тощо).

Методика та засоби пошуку й знешкодження радіозакладних пристроїв. За

наявності комплексу радіомоніторингу під час проведення таких робіт здійснюють моніторинг ефіру. У разі відсутності такого комплексу контроль здійснюють за допомогою сканера.

Дані роботи проводять зазвичай дві-три особи і завжди починаються із розпитувань власників приміщення, що перевіряється: чи дарували їм якісь сувеніри, якщо так, то коли, й які з них знаходяться у приміщенні? Далі проводять візуальний огляд приміщення, звертаючи особливу увагу на зручні (для розміщення закладки) місця. У цих роботах слід користуватися ліхтариком. Крім меблів, слід оглянути електричні та телефонні розетки, вентиляційні отвори, ніші для батарей опалювання тощо. Також особливу увагу слід звернути на рамки від різних картин, портретів, фотографій тощо. Під час їх огляду детально аналізують їх конструкцію та перевіряють, чи не виконані вони так, що утворюють резонансний контур для ВЧ-нав'язування. Далі, за допомогою сканера, перевіряють ефір. При цьому для активації закладок, що спрацьовують від акустичного сигналу, застосовують спеціальні сигнали, записані на магнітофон. Така фонограма записується з суміші мовних та синусоїдальних сигналів з частотою 400 Гц та 1 кГц.

Одночасно ведеться перевірка близького поля. Для цього застосовують індикатори (або детектори) поля. Такі прилади фіксують наявність джерела випромінювання, яке розташовано на відстані до 25 см від антени апарата. Це портативний широкосмуговий радіоприймач, що реагує на електромагнітне поле (джерело радіовипромінювання).

Як правило, такі прилади забезпечені світовою та звуковою індикацією, яка сигналізує про наближення до джерела випромінювання. Часто вони мають вбудований частотомір з індикацією частоти випромінювання. Такі прилади є незамінними там, де неможливо провести візуальний контроль.

Окрім цього необхідно провести комплексну перевірку електромережі, телефонної мережі на відсутність закладних пристроїв, що від них живляться, та інфрачервоних джерел випромінювання (зокрема, телевізійних камер).

Для виявлення закладок, які керуються дистанційно та можуть бути відключеними від джерела живлення на час перевірки, слід застосувати так званий нелінійний локатор, тобто апарат, який виявляє напівпровідникові прилади навіть якщо вони не працюють. За допомогою такого апарату слід перевірити усі предмети інтер'єру, стіни, стелю (особливо, якщо вона підвісна), підлогу (особливо паркетну). Апаратура цього типу побудована на властивій всім напівпровідникам нелінійності характеристик, отже на обов'язковому процесу нелінійного перетворення сигналів (модуляції), що на них подаються у

будь-який спосіб. Тому такі апарати випромінюють імпульси (або змінне електромагнітне поле достатньої потужності) та приймають і аналізують сигнал відгуку на наявність у ньому нових частотних складових, що відповідають другій та третій гармонікам контрольного сигналу.

Окрім виявлення радіозакладних пристроїв їх можна придушити шляхом встановлення активної радіотехнічної широкосмугової або прицільної (вузькосмугової) завади. Вузькосмугова завада ставиться у тому випадку, коли точно відомо частоту, на якій працює радіозакладка. Але цей спосіб захисту використовується досить рідко та лише у тому випадку, коли передавач закладки має дуже велику потужність.

Варто зауважити, що прилади постановки радіотехнічної завади володіють ще одним важливим призначенням. Їх застосовують для блокування радіовибухових пристроїв під час розмінування.

10.4 Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами

З розгляду методів та засобів зняття інформації стає зрозумілим про яку кількість каналів витоку іде мова, та як вони формуються на різноманітних технічних засобах, що застосовуються у робочих приміщеннях та у побуті. Стає зрозуміло, що під час проектування системи захисту інформації слід потурбуватися про їх блокування цих каналів.

Найбільш імовірне їх використання – це зняття акустичної та електромагнітної інформації. Найчастіше використовуються механізми перетворень акустичних сигналів у електричні та паразитні випромінювання і наведення. Також, варто пам’ятати про те, що ніколи не можна виключати можливість використання супротивником ВЧ-нав’язування.

Для блокування таких каналів витоку використовуються активні методи протидії. Блокувати такі канали витоку можна застосуванням активної завади у радіотехнічному та звуковому діапазоні частот. При цьому слід забезпечити можливість виконання технічними засобами, які треба захистити, своїх основних функцій без перешкод для їх роботи з боку засобів захисту інформації.

Для цього у різних країнах на різних етапах розвитку методів та засобів технічного захисту інформації розроблялися окремі прилади, використання яких вимагало узгодження їх різних характеристик та можливостей для отримання цілісного комплексу захисту інформації.

На сьогодні, у відповідності до ТУ У 31.6-33694400-002:2009, розроблено комплекс, який призначено для захисту інформації від витоку по провідникових

лініях електроживлення, пожежної та охоронної сигналізації, радіо- та телефонної мереж тощо. До складу цього комплексу входить ряд приладів, зокрема:

– роздільні трансформатор різної потужності;

– прилади захисту інформації в електромережі із придушенням небезпечних сигналів у смузі частот від 180 Гц до 30 МГц;

– генератор шуму у звуковому діапазоні частот;

– генератор шумоподібного сигналу для електромережі у діапазоні частот від 20 кГц до 1 ГГц;

– фільтр загороджувальний високих частот в слабкострумових лініях, який призначено для захисту таких ліній від проходження сигналів ВЧ-нав'язування;

– генератор шумоподібного сигналу у мовному діапазоні у слабкострумових лініях, який забезпечує активне маскування сигналу паразитного акустоелектричного перетворення у мовному частотному діапазоні у слабкострумових лініях;

– генератори шумоподібного радіочастотного сигналу у лініях аналогового телефонного зв'язку та у слабкострумових лініях.

Всі прилади, які входять до складу цього комплексу, побудовано на одній елементній базі та на одному загальному принципі. У більшості з них є вбудовані пристрої автоматизованого контролю працездатності.

Для активного захисту інформації від ВЧ-нав'язування використовують принципово новий метод, який було запропоновано О. В. Рибальським. Його застосування змінює властивості сигналу ВЧ-нав'язування, які робить його непридатним для отримання акустичної інформації. Цей ефект виникає тому, що випромінюється спеціальний сигнал протидії з частотою, яка близька до частоти сигналу зондування ВЧ-нав'язування. Це призводить до виникнення явища биття між цими сигналами, а при наближенні частоти випромінюваного сигналу протидії до частоти сигналу ВЧ- нав'язування відбувається навіть захоплення частоти сигналу протидії генератором сигналу зондування ВЧ-нав'язування. В результаті взаємодії двох таких коливань виникає нове коливання з частотою:

$$\omega=(\omega_1+\omega_2)/2,$$

де ω_1 – частота сигналу протидії;

ω_2 – частота сигналу зондування,

та змінною амплітудою, максимальні значення якої повторюються з частотою:

$$\Omega=\omega_1-\omega_2.$$

При цьому, при переході амплітуди цих коливань через нуль відбувається змінювання їх фази.

Під час використання ВЧ-нав'язування зняття інформації може відбуватися методами амплітудної, частотної та фазової модуляції. Сам факт виникнення нового коливання з іншою частотою вже перешкоджає зняттю інформації, оскільки не відбувається перевипромінювання модульованих інформацією сигналів, або їх рівень значно послаблюється.

Змінювання фази нового коливання перешкоджає зняттю інформації методом фазової модуляції. Але цей ефект підвищується для фазової та частотної модуляції за рахунок змінювання частоти генерації випромінюваного сигналу вліво та вправо від її середнього значення сигналом керування, складеним з випадковим сигналом.

Варто зауважити, що при цьому виникає паразитна амплітудна модуляція перевипромінюваних сигналів. А складання генерованого сигналу з іншим випадковим сигналом призводить до ще більшого рівня завад для амплітудної модуляції, що додатково перешкоджає зняттю інформації.

10.5 Захист інформації від несанкціонованого запису звукозаписувальними пристроями

Захист інформації від такого виду несанкціонованого зняття стає дедалі актуальнішим. При цьому слід виділити два напрямки захисту:

– виявлення у відвідувача або в приміщенні диктофона;

– придушення можливості запису на аналоговий апарат або на апарат цифрового звукозапису.

Виявлення звукозаписувального приладу у відвідувача може бути проведено звичайним детектором металу, але для цього його треба піддати явному контролю. Якщо така дія є небажаною, то можна скористатися індикаторним приладом наявності диктофону. Такий прилад зазвичай розташовують на одязі або тілі особи, яка здійснює перевірку. При наближенні на відстань від 0,5 до 1 м до працюючого диктофону прилад починає вібрувати

Для придушення можливості несанкціонованого запису інформації використовуються як прилади із випромінюванням акустичної завади, так і прилади із застосуванням електромагнітної завади.

За використання таких приладів слід пам'ятати, що вони випромінюють електромагнітне поле великої інтенсивності. Тому час роботи із такою апаратурою повинен бути обмеженим та не перевищувати 1…2 години на добу.

10.6 Захист електронної інформації

Проблемам захисту електронної інформації на сьогодні відведено дуже багато уваги як відкритого, так і спеціального характеру. Проведення таких робіт вимагає застосування спеціального обладнання та засобів вимірювальної техніки, які є лише на крупних спеціалізованих підприємствах радіоелектронного профілю. Як правило, вони мають ліцензії на виконання таких робіт та виконують їх на замовлення інших установ.

Основні методи, які використовують для захисту від витоку інформації із електронної, офісної та обчислювальної техніки:

– екранування паразитних випромінювань та наведень;
– маскування сигналів від паразитних випромінювань та наведень;
– застосування спеціальних ланцюгів заземлення;
– використання спеціальних джерел електроживлення;
– використання спеціальних фільтрів у мережах електроживлення;
– програмне шифрування інформації під час її запису на жорсткий диск або інший диск.

Усі ці роботи вимагають складного технологічного обладнання (наприклад, екранування комп'ютерної техніки відбувається за допомогою напилення тонких захисних шарів металу шляхом осадження у вакуумі). Захищаються таким чином корпуси системного блоку, монітору, магнітних та оптичних накопичувачів та інші блоки. Для маскування використовуються генератори широкосмугового шуму із спеціальним спектральним складом, який адаптується під кожний конкретний виріб.

Окрім цього, захищені засоби обробки інформації розміщуються у спеціальних приміщеннях із обмеженим доступом, а в самому приміщені встановлюється спеціальний додатковий пристрій – генератор випадкових електромагнітних коливань, які випромінюють їх в ефір та перешкоджають зняттю інформації із використанням паразитних випромінювань та наведень.

10.7 Захист письмової інформації від оптичного зняття

Зрозуміло, що отримати чужу письмову інформацію можна способом перлюстрації або звичайної крадіжки, тому питання боротьби із такими правопорушеннями варто розглядати у руслі захисту від оптичного зняття письмової інформації, яку можна зняти як з паперового носія, так і з екрану монітора комп'ютера.

Основними засобами захисту в такому разі будуть захист від зняття через вікна за допомогою фотографуючих та телевізійних пристроїв (відеокамер) із

спеціальними довгофокусними об'єктивами, так і за допомогою телекамер (відеокамер), розміщених у приміщенні.

Захист від оптичного зняття через вікна досягається або використанням спеціального скла (матового чи з нерівностями, що неуможливлюють перегляд приміщення), або застосуванням штор та спеціальних плівок, які наклеюють на скло.

Захист від телевізійних (відео) камер, які несанкціоновано встановлені всередині приміщення, досягається використанням приладів, що ставлять активну заваду роботі електронних приладів (що не завжди можливо), або пошуком, виявленням та знешкодженням таких пристроїв. Пошук телевізійних камер здійснюється тими самими приладами та за тією ж самою методикою, що й пошук радіозакладних пристроїв.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Що являє собою об'єкту технічного захисту інформації?
2. За яких умов застосовують комплексний захист інформації?
3. Основні та допоміжні технічні засоби.
4. Загроза для інформації. Рівень технічного захисту інформації.
5. Активний та пасивний захист інформації.
6. Порядок проведення робіт із технічного захисту інформації на об'єкті.
7. Які фізичні явища покладені у методи та засоби захисту акустичної інформації від витоку по вібраційних каналах?
8. Які прилади використовуються для захисту акустичної інформації?
9. Які прилади використовуються для виявлення засобів зняття акустичної інформації?
10. Методи виявлення радіозакладних пристроїв та їх візуальний пошук.
11. Які функції виконують програми моніторингу ефіру, сканери, індикатори електромагнітного поля та нелінійні локатори?
12. Які прилади застосовують для виявлення засобів зняття інформації?
13. ВЧ-нав'язування та генератори шуму.
14. Виявлення та захист акустичної інформації від несанкціонованого запису звукозаписувальними пристроями.
15. Які методи та засоби використовуються для захисту електронної та електромагнітної інформації?
16. Які технічні методи та засоби використовують для захисту письмової інформації?

Література: [2; 5-11; 14-17].

Тема 11. Методи та пристрої забезпечення захисту і безпеки

План:

11.1 Основні принципи захисту інформації при підключені до мережі Internet

11.2 Захист інформації за допомогою міжмережних екранів

11.3 Захист інформації на мережному рівні

11.4Застосування протоколів AH, ESP, SSL та TLS

11.1 Основні принципи захисту інформації при підключені до мережі Internet

Для підключення будь-якої організації до мережі Internet необхідно прийняти ряд певних організаційно-технічних заходів для її захисту.

При побудові захисту варто виходити з того, що будь-який захист ускладнює використання системи, що, за прямим призначенням обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вищим є захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів.

Тому, захищаючи мережу, варто виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що захищає. Існує ряд основних принципів, що дозволяють організувати досить безпечне підключення до Internet порівняно простими засобами.

Firewall (Брандмауер). Основним загальновизнаним засобом такого захисту є міжмережний екран. Брандмауер встановлюється між мережею та Internet і виконує роль мережного фільтра (рис. 11.1).

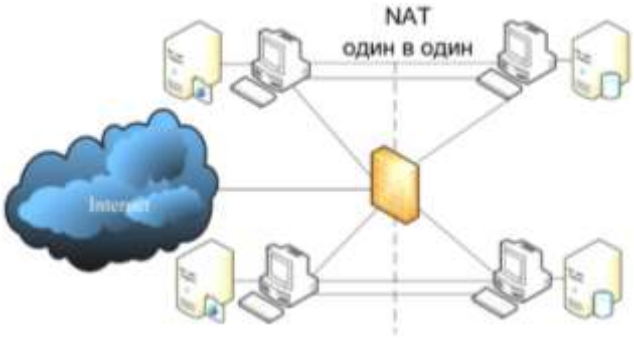

Рисунок 11.1 – Встановлення брандмауера у локальній мережі

Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Internet і назад, і обмежити трафік з боку Internet до мережі, яка потребує захисту, тільки необхідними службами, наприклад: smtp; dns; ntp.

Допустимість того або іншого трафіка визначається мережним адміністратором відповідно до політики інформаційної безпеки організації (наприклад, може бути дозволений доступ із частини комп'ютерів мережі до web- та ftp-серверів Internet і двонаправлений доступ між Internet та поштовим сервером, але при цьому заборонені всі інші протоколи й напрями трафіка).

Таким чином, міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора), логічно доцільно сполучити їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і безпосередньо сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак дане правило є необов'язковим і міжмережний екран може бути поданий окремим пристроєм.

У найпростішому випадку виконання функцій міжмережного екрана можна організувати за допомогою мережного фільтра на основі аркушів доступу (access-lists). Аркуші доступу визначають правила, за якими або дозволяється, або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. Як ознаки можуть використовуватися IP-адреси або діапазон, IP-адреса джерела й приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак IP-пакета.

Відмінність і недолік аркушів доступу порівняно із сьогоднішнім міжмережним екраном полягає у тому, що вони дозволяють створити статичний однобічний фільтр, тоді як мережне з'єднання становить динамічний процес. Аркуші доступу не дозволяють контролювати параметри IP-пакета, що залежать від попередніх пакетів. Звідси виникає складність застосування аркушів доступу для тонкого настроювання фільтрації трафіка в точній відповідності із прийнятою політикою безпеки. Зокрема, із цієї причини аркуші доступу не в змозі захистити від такого різновиду мережної атаки, як «викрадення з'єднання», або «хайджекінг».

У Firewall Feature Set зазначені проблеми вирішуються за допомогою того, що він відслідковує кожне мережне з'єднання окремо і контролює весь процес у динаміку. При встановленні нового TCP-сеансу міжмережний екран створює для нього новий процес, що контролює правильність з'єднання до самого моменту його завершення. При цьому кожний пакет на транспортному рівні перевіряється

на відповідність попередній, а всі «підозрілі» пакети відбраковуються. Завдяки цьому стає можливим досить легко організувати фільтр для доступу внутрішнього комп'ютера до зовнішнього, але не дозволяє зовнішньому комп'ютеру самостійно звернутися до внутрішнього.

Іншими словами, у настроюваннях міжмережного екрана задаються правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напряму й кожного тракту окремо. Якщо правило дозволяє проходження IP-пакета від інтерфейсу внутрішньої мережі до Internet-інтернетінтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який уже можуть пройти відповідні пакети від зовнішнього одержувача. Як тільки з'єднання закрите, або вичерпаний час очікування, тунель закривається, і обіг ззовні до внутрішнього комп'ютера буде відкинутий. З цієї ж причини екран не пропустить пакети у зворотному напрямі, якщо ініціатором з'єднання є зовнішній комп'ютер.

Окрім цього, міжмережний екран, на відміну від аркушів доступу, може контролювати зміст IP-пакетів у полі даних і відбраковувати пакети, що містять потенційно-небезпечні коди, наприклад, java-апліти. Є міжмережні екрани, здатні виявити в IP-пакетах ознаки відомих мережних атак і перервати таке з'єднання, але це вже досить дорогі системи.

NAT (Network Address Translation). Другою цеглинкою забезпечення захищеності мережі є «заміна мережної адреси» – NAT. Вона становить заміну в IP-пакеті реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні його в зовнішню мережу. Завдяки цьому для внутрішньої мережі стає можливим використання діапазонів адрес, які не застосовуються в Internet (наприклад, 10.0.0.0 – 10.255.255.255). Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп'ютерів і приховує структуру мережі. А практиці існують декілька різновидів NAT.

Найпростіша й найбільш трудомістка з огляду на захист – трансляція фіксованої внутрішньої адреси у фіксовану зовнішню. При цьому зловмисник безперешкодно «бачить» такий комп'ютер у зовнішній мережі, тому що йому однозначно відповідає певна зовнішня адреса. Однак вона необхідна при організації сервера, до якого необхідно забезпечити доступ ззовні (рис. 11.2).

Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. При цьому всі внутрішні комп'ютери можуть працювати з Інтернетом одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за службовими даними TCP-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно

ускладнює життя зловмиснику, тому що повністю приховує внутрішні комп'ютери й перешкоджає «визначенню жертви» (рис. 11.3). Зловмисник, навіть бачучи трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить. Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої адреси до внутрішньої. Зокрема виключається можливість сканування ззовні внутрішньої мережі.

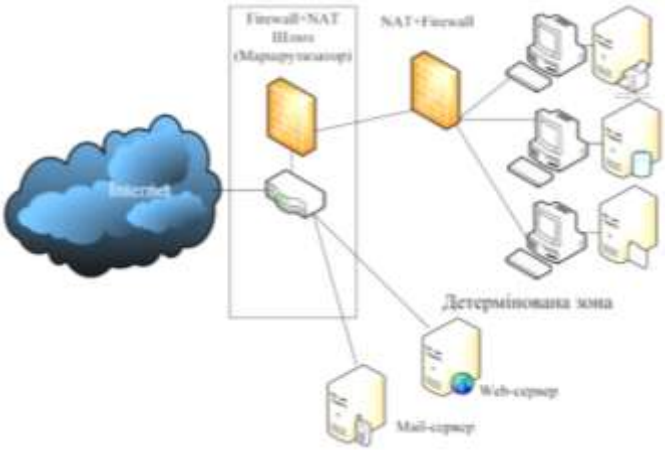

Рисунок 11.2 – Трансляція фіксованої внутрішньої адреси у фіксовану зовнішню

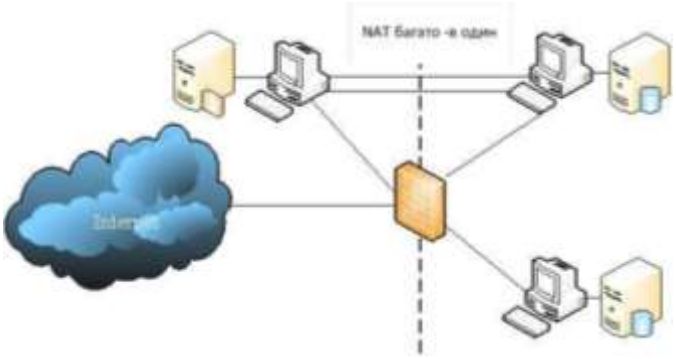

Рисунок 11.3 – Трансляція групи внутрішніх адрес в одну зовнішню

Третя форма NAT – використання для заміни внутрішніх адрес не однієї адреси, а будь-якої з виділених адрес. Тобто внутрішній комп'ютер, виходячи в

Інтернет, одержує вільну у цей момент адресу з бази даних (БД). При цьому адреси підмінюються динамічно, і кожне нове TCP-з'єднання може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі зловмиснику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно.

Сказане відносно другої форми NAT є справедливим і для третьої форми. Якщо запит приходить ззовні, то маршрутизатор не в змозі зв'язати адресу з БД з адресою мережі. Тому такий запит не досягне мети.

Демілітаризована зона. Як правило, організації потрібно мати у себе деякі мережні ресурси, до яких відкритий доступ з мережі Інтернет (зазвичай це поштовий, dns і web-сервери). Механізм їх роботи припускає, що до них повинен бути дозволений вільний або слабко обмежений доступ з Internet. Відповідно ймовірність їх зламу вища, у порівнянні із іншими комп'ютерами мережі. Із цих міркувань розташовувати їх усередині зони, яка захищається, недоцільно з точки зору безпеки, тому що у випадку зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів.

Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережним екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їх розміщення називають демілітаризованою зоною (рис. 10.4).

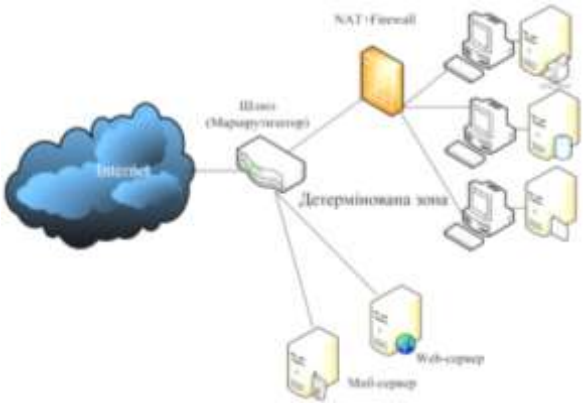

Рисунок 11.4 – Демілітаризована зона

Другий Firewall. З рисунка 11.4 видно, що ніщо не заважає встановити другий Firewall на основному шлюзі мережі. Це є логічним рішенням і дозволяє одночасно підвищити рівень захисту внутрішньої мережі й захистити сервери

демілітаризованої зони. За правильного налаштування обох міжмережних екранів зловмиснику буде вже набагато складніше дістатися до внутрішньої мережі. Наявність другого міжмережного екрана ускладнює конфігурацію мережевого устаткування й налаштування роботи усіх елементів мережі.

Для додаткового підвищення захищеності можна використати Firewall-и різних виробників. Тоді якщо в одному з них буде виявлена вразливість, інший не дозволить противнику безперешкодно проникнути у мережу, як це мало б місце при використанні Firewall-ів одного типу.

Варто підкреслити, що можливість мережевого доступу до шлюзів і до міжмережевих екранів, з метою уникнення зловмисного використання, повинна бути відключеною. З огляду безпеки пристрої, які знаходяться на охороні мережі, повинні конфігуруватися та адмініструватися тільки через консольний порт локально (рис. 11.5).

Рисунок 11.5 – Локально-консольний порт для серверів

Схема, запропонована на рисунку 11.5, може бути дещо вдосконалена. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами (рис. 11.6).

Proxy-сервер. Використання так званого «посередника» (proxy-сервера) також підвищує рівень захищеності мережі, тому що виключає необхідність прямого виходу в Internet комп'ютерів користувачів. При цьому також стає можливим більш строгий контроль за даними в IP-пакетах на рівні мережних додатків. Proxy-сервер працює як посередник між користувальницьким додатком

і вилученим мережним ресурсом в Internet. Схематично суть його роботи подано на рисунку 11.6.

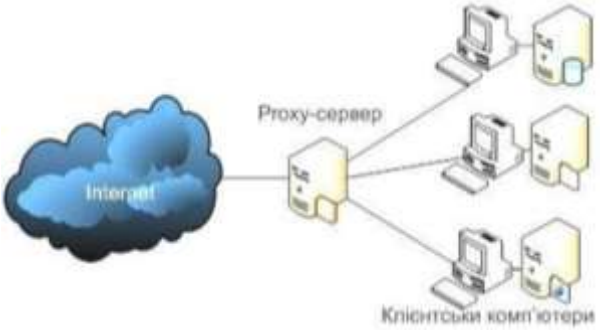

Рисунок 11.6 – Proxy-сервер

Proxy-сервер складається із двох частин – клієнтської та серверної. Клієнтська частина дивиться у бік Internet, серверна – у бік клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до вилученого сайта через proxy-сервер, його клієнтський мережний додаток взаємодіє із серверною частиною proxy-сервера. При цьому proxy-сервер на рівні додатка передає клієнтський запит своєї клієнтської частини, і вона вже від імені proxy-сервера надсилає даний запит на вилучений сайт. Тобто IP-пакет, що відправлений, має адресу proxyсервера.

Потім отримана відповідь передається у зворотну сторону від клієнтської частини proxy-сервера його серверної частини, з якою безпосередньо взаємодіє користувальницький комп'ютер. Таким чином, пряме з'єднання клієнтських комп'ютерів з вилученим сайтом виключається. Усередині proxy-сервера передача даних між клієнтською частиною й серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатка, ніж забезпечується легкість контролю команд і даних на відповідність установленим стандартам. Крім того, це дозволяє забезпечити досить надійний контроль проти передачі шкідливих кодів усередині даних. Навіть у випадку успішної атаки з боку Internet за відкритими протоколами у цьому випадку буде ушкоджений тільки proxyсервер, що не представляє інформаційної цінності, а користувальницькі комп'ютери будуть залишатися в безпеці ще якийсь час.

Через те, що proxy-сервер працює тільки за декількома відомими протоколами (HTTP, FTP тощо) і не пропускає через себе інші пакети, він сильно обмежує можливості зловмисника із використання мережевих

«троянських коней» для закріплення на будь-якому з користувальницьких комп'ютерів.

Другий mail-сервер. Залишати mail-сервер у демілітаризованій зоні з одного боку небажано, бо на ньому фактично зберігається поштова база даних з перепискою локальних користувачів, а демілітаризована зона не може забезпечити належного рівня захисту мережним ресурсам. З іншого боку, якщо сховати mail-сервер усередині локальної мережі, то він або не зможе взаємодіяти із зовнішнім середовищем, або буде становити ворота із зовнішнього середовища у внутрішню локальну мережу, якими потенційно зможе скористатися зловмисник.

Внаслідок цього доречним рішенням є використання двох поштових серверів. Основний сервер установлюється всередині мережі, яка захищена, і його не видно для зовнішнього світу. Всі локальні користувачі поштової системи заводяться на нього і мають до нього прямий доступ. Відповідно вся вхідна кореспонденція зберігається на ньому у поштових скриньках локальних користувачів. Відправлення електронної пошти також здійснюється через нього.

Другий, або зовнішній, поштовий сервер встановлюється в демілітаризованій зоні й забезпечує взаємодію по e-mail з мережою Internet. Він настроюється таким чином, щоб всю пошту, яка приходить на ім'я користувачів організації, відразу пересилати на внутрішній поштовий сервер. У такий спосіб у його поштовій базі даних немає ні одного облікового запису користувачів організації і жоден лист не відкладається для довгострокового зберігання. Тому якщо він виявиться зламаним зловмисником, то він не отримає доступу до накопиченої переписки. Проте після зламу зловмисник отримає можливість перехоплення й читання транзитної пошти. Тому ретельний контроль за подібною ситуацією є необхідним, що призводить до негайного вживання заходів під час виникнення підозри на несанкціонований доступ.

Перевагою такої схеми є те, що навіть зі зламаного зовнішнього поштового сервера не так просто дістатися до внутрішньої захищеної мережі. Обмін даними між зовнішніми й внутрішнім поштовими серверами відбувається через міжмережний екран з єдиним дозволеним портом (SMTP) за єдиною дозволеною парою адрес. Звернення до інших комп'ютерів і за іншими протоколами буде блокуватися. Тому впливати з нього прямо на комп'ютери користувачів внутрішньої мережі неможливо.

Антивірусний захист поштової системи. Операційна система Windows дуже вразлива перед деякими різновидами поштових вірусів. Користувачу буває досить встановити покажчик на інфікований лист, щоб вірус активізувався. Але

більш небезпечним є те, що механізм роботи поштових вірусів може бути використаний зловмисником для закидання в область мережевого «троянського коня», якими захищається. Він дозволить зловмиснику таємно скачувати дані мережі та здобути всю інформацію, яка його цікавить. Тому забезпечення антивірусного захисту трафіку доставки пошти у внутрішню мережу варто приділити достатньо серйозну увагу.

Існує ряд програмних засобів, призначених для контролю кореспонденції на поштових серверах на предмет наявності в ній вірусів у процесі прийому й пересилання електронної пошти.

Принцип її роботи полягає в тому, що уся пошта, яка проходить через сервер, спочатку перенаправляється спеціальному користувачу, у ролі якого виступає антивірусний процес. Він сканує зміст кожного листа на наявність у ньому фрагментів відомих вірусів. Якщо аркуш містить щось схоже на вірус, воно вилучається із процесу передачі й, залежно від настроювань антивірусу, піддається заданій обробці. Повідомлення про виявлений вірус відсилаються відправнику й одержувачу інфікованого листа, а також на ім'я зазначених адміністраторів системи. Після перевірки листи, які не викликають підозри, надсилаються за призначенням.

Тим самим на рівні поштового сервера вибудовується надійний захист відомим вірусам у електронній пошті. Через те, що антивірусна програма розпізнає тільки віруси, сигнатури яких перебувають у її базі даних, необхідно регулярно обновляти антивірусну базу даних з офіційного сайта. Інакше мережа може стати вразливою для знову створених вірусів.

Log-сервер. Log-сервер є загальновідомим механізмом протоколювання системних подій на серверах і клієнтських робочих станціях. Розробники програмного забезпечення включають у свої продукти фрагменти коду, які на ту або іншу подію генерують відповідні текстові повідомлення, які надсилаються операційній системі. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем з метою з'ясування, які події відбувалися в системі деякий час потому. Це дозволяє, наприклад, з'ясувати, чому не запускається та або інша програма, або чому припинив функціонувати певний сервіс. Дуже корисним log-файли є для пошуку слідів зламу системи й відвідування її несанкціонованими гостями. Через те, що злом, як правило, супроводжується множиною заборонених дій, це породжує велику кількість системних повідомлень, які й осідають в log-файлах.

Із цієї причини зловмисник завжди прагне стерти сліди своєї присутності шляхом видалення log-файлів, або їх підчищання. В обох випадках

адміністратору буде важко зрозуміти, що ж відбулося в системі насправді – яким чином у неї проникнули, як довго в ній перебували, перед тим як встигли покористуватися, або просто переконатися, що все добре.

Тому обов'язковою умовою для мережі, підключеної до Internet, є наявність у ній окремого log-сервера.

Принцип його роботи полягає в тому, що кожна операційна система може посилати повідомлення про системні події за UDP-протоколом на вилучений сервер. Це можуть робити також маршрутизатори й міжмережні екрани.

Збираючи такі повідомлення на спеціально виділеному сервері, забезпечується їм схоронність від рук зловмисника. Тому для мінімізації ймовірності зламу log-сервер повинен бути призначеним лише для збору log-повідомлень. Він не повинен виконувати будь-яких інші функції та виконувати інші мережні додатки, окрім syslogd.

У цьому випадку після зламу будь-яких комп'ютерів мережі на log-сервері залишаться відповідні повідомлення, знищити які противник уже не зможе. Таким чином, у результаті найбільш оптимальною є наступна схема підключення локальної мережі до Internet (рис. 11.7).

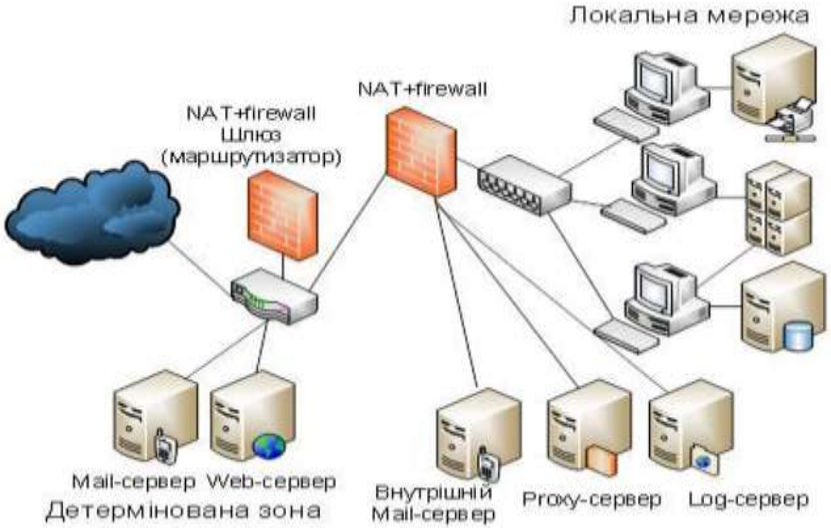

Рисунок 11.7 – Схема з Log-сервером

Таким чином, проведений аналіз способів захисту комп'ютерних мереж при підключені їх до глобальної мережі Інтернет вказує на те, що для забезпечення захисту під час обміну інформацією абоненти локальної мережі повинні

використовувати принципи і засоби безпеки в комплексі із організаційними заходами. Це дозволить надійно захистити від атак як активних, так і пасивних противників.

11.2 Захист інформації за допомогою міжмережних екранів

Серед програмно-апаратних і програмних засобів забезпечення автентичності, розподілених комп'ютерних мереж (КМ), можна виділити міжмережеві екрани (ММЕ), засоби аналізу захищеності й засоби виявлення атак.

Міжмережеві екрани (брандмауери, firewall) реалізують набір правил, які визначають умови проходження пакетів даних з однієї частини розподіленої КМ (відкритої) в іншу (захищену). Залежно від рівня взаємодії об'єктів мережі основними різновидами ММЕ є фільтруючі маршрутизатори, шлюзи сеансового й прикладного рівнів. Основною функцією фільтруючих маршрутизаторів, що працюють на мережному рівні еталонної моделі, є фільтрація пакетів даних, які входять у захищену частину мережі або вихідних з неї. Правила фільтрації визначають, дозволяється або блокується проходження через ММЕ пакета із правилами, які задаються цими параметрами.

До основних переваг фільтруючих маршрутизаторів відносяться:

– простота їх створення, установка й конфігурування;

– прозорість для додатків користувачів КМ і мінімальний вплив на їх продуктивність;

– невисока вартість.

Недоліками фільтруючих маршрутизаторів є:

– відсутність автентифікації на рівні користувачів КМ;

– уразливість для підміни IP-адреси в заголовку пакета;

– незахищеність від погроз порушення конфіденційності й цілісності переданої інформації;

– сильна залежність ефективності набору правил фільтрації від рівня знань адміністратора ММЕ конкретних протоколів;

– відкритість IP-адрес комп'ютерів захищеної частини мережі.

Шлюзи сеансового рівня призначені для контролю віртуального з'єднання між робочою станцією захищеної частини мережі й хостом її незахищеної частини і трансляції IP-адрес комп'ютерів захищеної частини мережі.

У процесі виконуваного шлюзом сеансового рівня процедури трансляції IP-адрес відбувається їхнє перетворення в одну IP-адресу, асоційовану із ММЕ. Це виключає пряму взаємодію між хостами захищеної й відкритої мереж і не

дозволяє порушнику здійснювати атаку шляхом підміни IP-адрес.

До переваг шлюзів сеансового рівня відносяться їх простота й надійність програмної реалізації. Недоліком є відсутність можливості перевіряти вміст переданої інформації. Це дозволяє порушнику намагатися передати пакети зі шкідливим програмним кодом і звернутися потім прямо до одного із серверів, що атакується КМ.

Шлюзи прикладного рівня не тільки виключають пряму взаємодію між уповноваженим користувачем із захищеної частини мережі й хостом з її відкритої частини, але й фільтрують усі вхідні й вихідні пакети даних на прикладному рівні (на основі аналізу змісту переданих даних).

Основні функції шлюзів прикладного рівня:

– ідентифікація й автентифікація користувача КМ при спробі встановити з'єднання;

– перевірка цілісності переданих даних;

– розмежування доступу до ресурсів захищеної й відкритої частин розподіленої КМ;

– фільтрація і перетворення переданих повідомлень (виявлення шкідливого програмного коду, шифрування й розшифрування тощо);

– реєстрація подій у спеціальному журналі;

– кешування запитуваних ззовні даних, розміщених на комп'ютерах внутрішньої мережі (для підвищення продуктивності КМ).

Перевагами шлюзів прикладного рівня також є:

– прихованість структури захищеної частини мережі для інших хостів;

– надійна автентифікація й реєстрація минаючих повідомлень;

– більш прості правила фільтрації пакетів на мережному рівні, відповідно до яких маршрутизатор повинен пропускати тільки трафік, призначений для шлюзу прикладного рівня, і блокувати весь інший трафік;

– можливість реалізації додаткових перевірок.

Основними недоліками шлюзів прикладного рівня є більш висока вартість, складність розробки, установки й конфігурування, зниження продуктивності КМ, «непрозорість» для додатків користувачів КМ.

Міжмережеві екрани є основою для створення віртуальних приватних мереж (Virtual Private Network, VPN), які призначені для приховання топології внутрішніх мереж організацій, що обмінюються інформацією з мережею Інтернет, і захисту трафіка між ними. При цьому використовуються спеціальні системи маршрутизації.

Загальним недоліком ММЕ будь-якого виду є те, що ці програмно-апаратні

засоби захисту в принципі не можуть запобігти багатьох видів атак (наприклад, загрози несанкціонованого доступу до інформації з використанням неправильного сервера служби доменних імен мережі Інтернет, загрози аналізу мережного трафіка, загрози відмови в обслуговуванні). Порушнику реалізувати загрозу доступності інформації в КМ, що використовує ММЕ, може виявитися навіть простіше, тому що досить атакувати тільки хост із ММЕ для фактичного відключення від зовнішньої мережі всіх комп'ютерів захищеної частини мережі.

11.3 Захист інформації на мережному рівні

Internet Protocol Security (IPSec) – це узгоджений набір відкритих стандартів, який має на сьогоднішній день конкретну специфікацію, і в той же час, може бути доповненим новими протоколами, алгоритмами та функціями мережевої безпеки.

Основне призначення протоколів IPSec – забезпечення безпечної передачі даних IP-мережами. Їх застосування забезпечує:

– цілісність, тобто здатність телекомунікаційної мережі забезпечувати передачу даних без спотворення, втрати або дублювання;

– автентичність, тобто здатність телекомунікаційної мережі забезпечувати передачу даних з можливістю підтвердити їх достовірність, тобто дійсність того, що дані передані саме тим відправником, за кого він себе видає;

– конфіденційність, тобто здатність телекомунікаційної мережі забезпечувати передачу даних у формі, що запобігає їх несанкціонованому перегляду.

Специфікація IP Security (більш відома як IPSec) розробляється робочою групою IP Security Protocol IETF. Спочатку IPsec включала у себе 3 алгоритмо-незалежні базові специфікації, опубліковані в якості RFCдокументів «Архітектура безпеки IP», «Автентифікований заголовок (AH)», «Інкапсуляція зашифрованих даних (ESP)» (RFC1825, 1826 і 1827). В кінці 1998 року робоча група IP Security Protocol запропонувала нові версії цих специфікацій, які мають на даний час статус попередніх стандартів, це RFC2401…RFC2412.

Версії RFC1825-27 впродовж останніх декількох років вважаються застарілими і реально не використовуються. Робоча група IP Security Protocol розробляє також і протоколи управління ключовою інформацією. Завданнями цієї групи є розробка Internet Security Association and Key Management Protocol (ISAKMP), протоколу управління ключами прикладного рівня, не залежного від використовуваних протоколів забезпечення безпеки.

Основними компонентами IPsec є:

– RFC2402 «IP Authentication Header» (AH), призначений для контролю цілісності та автентичності пакетів даних в IP-мережах;

– RFC2406 «IP Encapsulation Security Payload» (ESP), призначений для забезпечення конфіденційності, контролю цілісності та автентичності пакетів даних у IP-мережах;

– RFC2408 «Internet Security Association and Key Management Protocol» (ISAKMP), призначений для забезпечення узгодження параметрів, створення, зміни, знищення контекстів захищених з'єднань (Security Association, SA) і управління ключами в IP-мережах;

– RFC2409 «The Internet Key Exchange» (IKE), є подальшим розвитком і адаптацією ISAKMP, призначений для роботи з протоколами IPSec.

Ядро IPSec складають три протоколи (рис. 11.8):

– протокол автентичності (Authentication Header, AH);

– протокол шифрування (Encapsulation Security Payload, ESP);

– протокол обміну ключами (Інтернет Key Exchange, IKE).

Рисунок 11.8 – Основні компоненти протоколу мережевої безпеки IPSec

Функції з підтримання захищеного каналу розподіляються між цими протоколами таким чином:

– протокол AH забезпечує цілісність і автентичність даних;

– протокол ESP шифрує дані, що передаються, гарантуючи конфіденційність, але він також може підтримувати автентифікацію та цілісність даних;

– протокол IKE вирішує допоміжну задачу автоматичного надання секретних ключів, необхідних для роботи протоколів автентифікації і шифрування даних.

Можливості протоколів AH та ESP частково перекриваються. Протокол AH відповідає тільки за контроль цілісності і автентифікації даних, в той час, як протокол ESP дозволяє шифрувати дані, й виконувати функції протоколу AH (в обмеженому вигляді). Для забезпечення цілісності та автентифікації пакетів даних використовуються спеціальні механізми контролю цілісності та автентичності, які засновані присвоєнням у дані, які передаються спеціально сформованої надмірності (коди контролю цілісності та автентичності).

Для забезпечення ефективного функціонування протоколів AH і ESP використовується протокол IKE, який встановлює між двома кінцевими точками логічне з'єднання, яке в IPSec носить назву «безпечна асоціація» (Security Association, SA).

Встановлення SA починається із взаємної автентифікації сторін. Обрані далі параметри SA визначають, який з двох протоколів, AH або ESP, застосовується для захисту даних, які функції виконує протокол захисту: наприклад, тільки автентифікацію та перевірку цілісності або, крім того, ще й захист від помилкового відтворення.

Протоколи AH і ESP забезпечують захист даних у двох режимах: транспортному і тунельному (рис. 11.9 та 11.10).

Рисунок 11.9 – Схема захисту пакета даних у транспортному режимі функціонування протоколів AH і ESP

У транспортному режимі (рис. 11.9) передача IP-пакета виконується за допомогою оригінального заголовка цього пакета даних. Перевагою такого

режиму є істотно менші обчислювальні та комунікаційні витрати. В той же час, з точки зору забезпечення безпеки телекомунікаційної мережі, для транспортного режиму функціонування протоколів AH і ESP притаманні такі недоліки: протокол ESP в транспортному режимі не захищає заголовок пакета даних; неможливо приховати топологію мережі, оскільки заголовки пакетів даних передаються у відкритому (не захищеному) вигляді.

У тунельному режимі (рис. 13.10) вихідний IP-пакет розташовується у новому, після чого здійснюється передача даних мережою виконується на підставі заголовка нового IP-пакета.

Рисунок 11.10 – Схема захисту пакета даних у тунельному режимі функціонування протоколів AH і ESP

Цей режим забезпечує захист заголовка пакета даних, у результаті чого ховається топологія мережі, що є безумовною перевагою під час побудови захищених телекомунікаційних систем і мереж.

У тож же час реалізація тунельного режиму вимагає великих обчислювальних і комунікаційних ресурсів. Застосування того чи іншого режиму залежить від вимог, які висуваються до захисту даних, а також від ролі, яку відіграє в мережі вузол, завершальний захищений канал. Так, вузол може бути хостом (кінцевим вузлом) або шлюзом (проміжним вузлом). На практиці використовують три схеми застосування IPSec:

– «хост-хост» (рис. 11.11);
– «шлюз-шлюз» (рис. 11.12);
– «хост-шлюз» (рис. 11.13).

У першій схемі захищений канал (безпечна асоціація, SA), встановлюється між двома кінцевими вузлами телекомунікаційної мережі. Протокол IPSec в

цьому випадку працює на кінцевому вузлі та захищає дані, які надходять до нього. Для схеми «хост-хост» найчастіше використовується транспортний режим захисту, хоча дозволяється і тунельний.

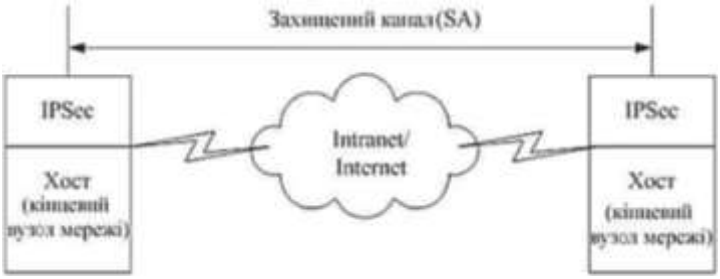

Рисунок 11.11 – Схема організації захищеного каналу «хост-хост»

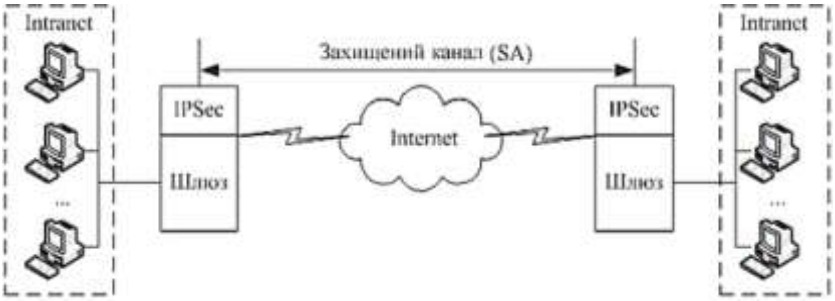

Рисунок 11.12 – Схема організації захищеного каналу «шлюз-шлюз»

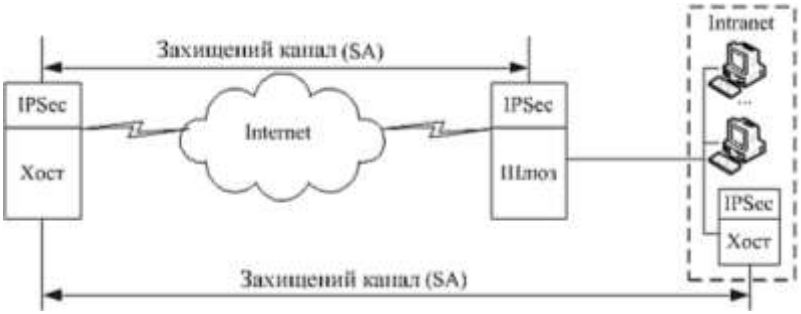

Рисунок 11.13 – Схема організації захищеного каналу «хост-шлюз» з додатковим каналом «хост-хост»

Відповідно до другої схеми, захищений канал встановлюється між двома проміжними вузлами, так званими шлюзами безпеки (Security Gateway, SG), на

кожному з яких працює протокол IPSec. Захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібна, вони передають свій трафік у незахищеному вигляді через мережу Intranet. Трафік, що направляється в загальнодоступну мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою IPSec, діючи від свого імені. Шлюзи можуть використовувати тільки тунельний режим роботи.

Схема «хост-шлюз» часто застосовується при віддаленому доступі. Тут захищений канал організовується між віддаленим хостом, на якому працює IPSec, і шлюзом, який захищає трафік для всіх хостів, які входять до складу внутрішньої мережі Intrenet установи. Віддалений хост може використовувати під час відправлення пакетів шлюзу як транспортний, так і тунельний режим, в свою чергу шлюз відправляє пакет хосту тільки в тунельному режимі. Цю схему можна ускладнити, створивши паралельно ще один захищений канал – між віддаленим хостом і яким-небудь іншим хостом, який належить внутрішній мережі та захищається шлюзом. Таке комбіноване використання двох SA дозволяє надійно захистити трафік і у внутрішній мережі.

13.4 Застосування протоколів AH, ESP, SSL та TLS

Забезпечення цілісності та автентичності даних в IP-мережах із використанням протоколу AH (IPSec). Автентифікований заголовок (AH) є звичайним опційним заголовком і, як правило, розташовується між основним заголовком пакета IP і полем даних. Наявність AH ніяк не впливає на процес передачі інформації транспортного і більш високого рівнів. Основним і єдиним призначенням AH є забезпечення контролю цілісності та автентичності пакетів даних для захисту від атак, пов’язаних з несанкціонованою зміною вмісту пакета, і в тому числі від підміни вихідного адреси мережевого рівня.

Протоколи більш високого рівня необхідно модифікувати з метою здійснення перевірки автентичності отриманих даних. Формат AH, який наведено на рисунку 11.14, складається із 96-бітового заголовка і даних змінної довжини, які формуються з 32-бітових слів. Назви полів достатньо ясно відображають їх вміст:

- Next Header – вказує на наступний заголовок;
- Payload Len – представляє довжину пакета;
- SPI – покажчик контексту безпеки;
- Sequence Number Field – містить послідовний номер пакета.

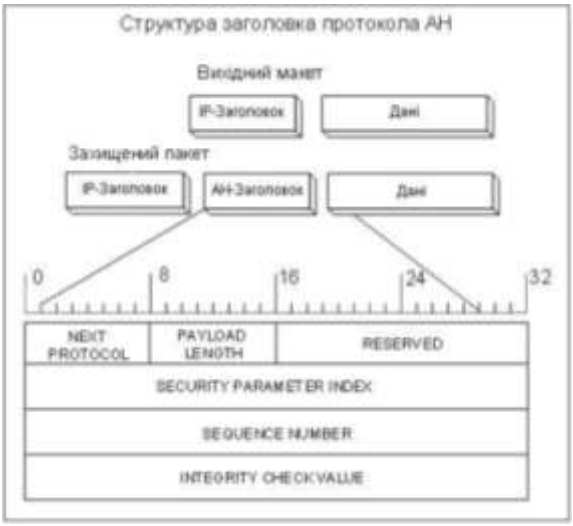

Рисунок 11.14 – Формат заголовка AH

На відміну від алгоритмів обчислення контрольної суми, які використовуються у протоколах передачі інформації комутованими лініями зв'язку або каналами локальних мереж і орієнтовані на виправлення випадкових помилок середовища передачі, механізми контролю цілісності та автентичності даних призначені для захисту від внесення цілеспрямованих змін. Застосування механізмів контролю цілісності та автентичності для кожного IP-пакета є ефективним засобом боротьби з атаками типу перехоплення, модифікації трафіку і підміни IP-адрес.

Окрім цього, забезпечується захист від повторної передачі пакетів у IP-мережах. При цьому реалізація протоколу AH не припускає забезпечення конфіденційності даних, тобто інформаційні дані кожного пакета передаються в незашифрованому вигляді.

Як видно із розглянутої структури заголовка AH при розрахунку значень кодів контролю цілісності та автентичності пакетів даних (Integrity Check Value, ICV) не використовуються змінні IP-заголовки оригінального пакета. Заголовок AH збільшує довжину оригінального IP-пакета приблизно на 24 байти (196 біт), основну частину цих додатковонесених надлишкових даних займає код контролю цілісності та автентичності ICV.

Для формування кодів контролю цілісності та автентичності ICV використовуються спеціальні механізми безпеки інформації:

– коди виявлення маніпуляцій (MDC – Manipulation Detection Code);

– коди автентифікації повідомлень (MAC – Message Authentication Code).

Їх формування засноване на використанні функцій гешування, які дозволяють для даних у загальному випадку довільної довжини формувати геш-код (геш-значення) строго заданої довжини.

Зазначені механізми застосовуються за замовчуванням, з метою забезпечення цілісності та автентичності пакетів даних для усіх реалізацій мереж IPv6. При цьому для формування ICV в протоколі AH передбачено обов'язкові алгоритми (для забезпечення сумісності програмних продуктів різних виробників):

– HMAC-MD5-96 – описаний в стандарті RFC 2403;
– HMAC-SHA-1-96 – описаний в стандарті RFC 2404.

Орім цього, передбачено й деякі інші алгоритми для формування ICV.

Специфікацією протоколу AH передбачено також використання нових, більш ефективних алгоритмів формування ICV, які розробляються або будуть розроблені в найближчому часі, що дозволяє говорити про високу гнучкості протоколу AH і простоті його подальшої модернізації.

Протокол AH може використовуватися як у тунельному, так і в транспортному режимах, самостійно та у комбінації із протоколом ESP.

Забезпечення конфіденційності, цілісності та автентичності даних у IP-мережах з використанням протоколу ESP (IPSec). У разі використання інкапсуляції зашифрованих даних заголовок ESP є останнім у ряду опційних заголовків, «видимих» у пакеті. Формат ESP (рис. 11.15) так само, як і формат AH, може зазнавати значні зміни залежно від застосованих криптографічних алгоритмів. Проте, у форматі ESP можна виділити такі обов'язкові поля: SPI, яке вказує на контекст безпеки і Sequence Number Field, що містить послідовний номер пакета.

Поле «ESP Authentication Data» (контрольна сума), не є обов'язковим в заголовку ESP. Одержувач пакета ESP розшифровує ESP заголовок і використовує параметри і дані застосованого алгоритму шифрування для декодування інформації транспортного рівня.

Протокол ESP реалізує: шифрування даних IP-пакетів для забезпечення конфіденційності інформації; додатково (аналогічно до протоколу AH) автентифікацію джерела кожного пакета, цілісність даних кожного пакета, захист від повторної передачі пакетів.

Заголовок ESP так само, як і заголовок AH збільшує довжину оригінального IP-пакета приблизно на 24 байти (196 біт), основну частину цих додатково внесених надлишкових даних займає код контролю цілісності та автентичності

ESP. Для його формування в протоколі ESP передбачено використання спеціальних механізмів контролю цілісності та автентичності даних (аналогічні тим, які використовуються протоколом AH) з можливістю заміни їх на більш ефективні.

Рисунок 11.15 – Формат заголовка ESP

Для забезпечення конфіденційності даних IP-пакетів передбачено використання криптографічних алгоритмів шифрування, серед яких передбачені обов'язкові алгоритми (для забезпечення сумісності програмних продуктів різних виробників), такі, наприклад, як DES-CBC (описаний в стандарті RFC 2405), NULL (описаний в стандарті RFC 2410).

Окрім цього, передбачено деякі інші (додаткові) алгоритми шифрування, наприклад, CAST-128, IDEA, 3DES (описані в стандарті RFC 2451), а також національний стандарт шифрування США AES-128, 192, 256 (FIPS-197).

Протокол ESP може використовуватися як в тунельному, так і в транспортному режимах, самостійно й в комбінації із протоколом AH.

Застосування протоколів AH і ESP в транспортному та тунельному режимах. Транспортний режим використовується для захисту поля даних IP-пакета, який містить протоколи транспортного рівня (TCP, UDP, ICMP), що, у свою чергу, містить інформацію прикладних служб.

Схему проходження IP-пакета даних з використанням протоколів безпеки AH і ESP в транспортному режимі наведено на рисунку 11.16. Прикладом застосування транспортного режиму є передача електронної пошти. Всі проміжні вузли на маршруті пакета від відправника до одержувача

використовують тільки відкриту інформацію мережевого рівня і, можливо, деякі опційні заголовки пакета (в IPv6).

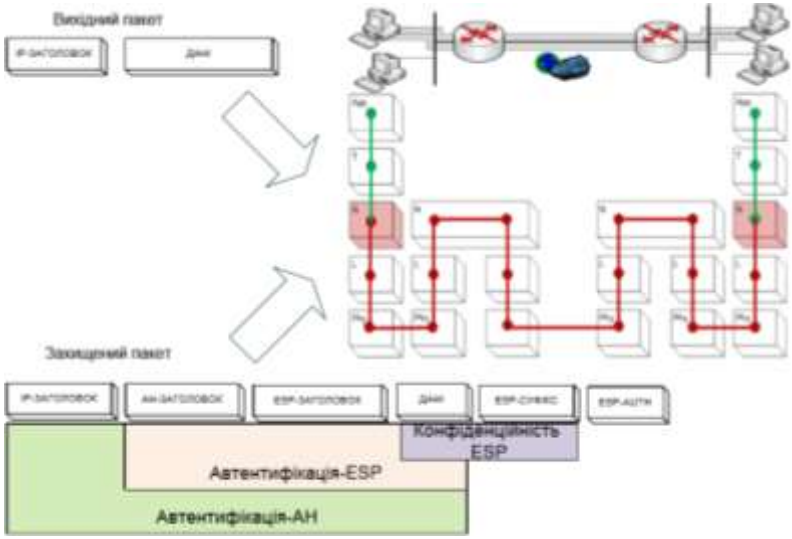

Рисунок 11.16 – Схема проходження IP-пакета даних з використанням протоколів безпеки AH і ESP в транспортному режимі

Недоліком транспортного режиму є відсутність механізмів приховання конкретного відправника й отримувача пакета, а також можливість проведення аналізу трафіку. Результатом такого аналізу може стати інформація про об'єми і напрями передачі інформації, області інтересів абонентів, розташування керівників.

Тунельний режим (рис. 11.17) передбачає захист (у тому числі шифрування) всього пакета, включаючи заголовок мережевого рівня. Тунельний режим застосовується у разі потреби приховання інформаційного обміну організації із зовнішнім світом. При цьому, адресні поля заголовка мережевого рівня пакета, що використовує тунельний режим, заповнюються міжмережевим екраном організації і не містять інформації про конкретного відправника пакета.

Під час передачі інформації із зовні мережі в локальну мережу установи за адресу призначення використовують мережеву адреса міжмережевого екрану. Після розшифрування міжмережевим екраном початкового заголовка мережевого рівня пакет направляється одержувачу.

Таким чином, проведений аналіз сучасних протоколів мережевої безпеки, які застосовуються в IP-мережах для забезпечення цілісності, автентичності та

конфіденційності передачі даних, дозволяє зробити наступні висновки: застосування механізмів захисту інформації на верхніх рівнях (рівня прикладного процесу, рівня представлень або сеансового рівня) моделі OSI дозволяє ефективно реалізувати функції безпеки конкретних мережевих служб. Такий спосіб захисту інформації не залежить від того, які мережі (IP або IPX, Ethernet або ATM) застосовуються для транспортування даних, що є безперечною перевагою такого підходу.

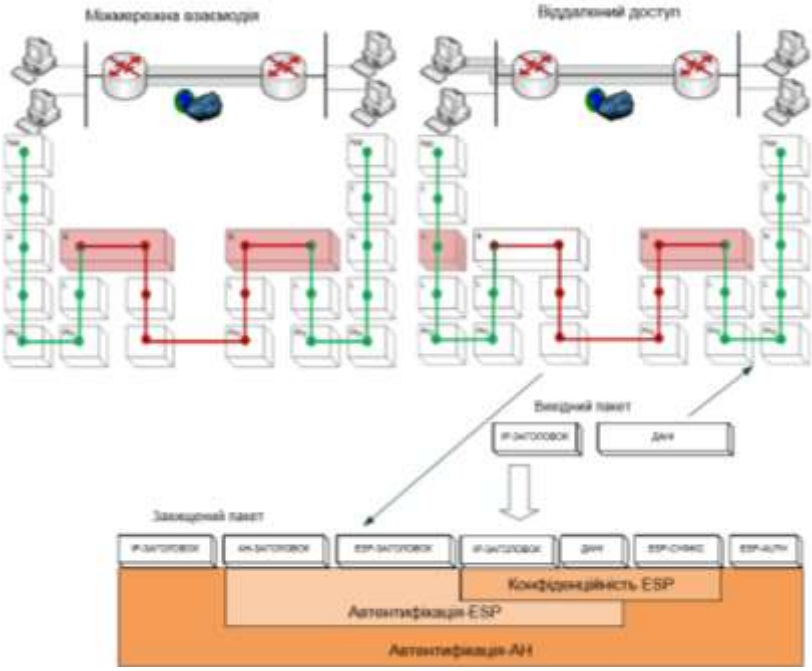

Рисунок 11.17 – Схема проходження IP-пакета даних з використанням протоколів безпеки AH і ESP в тунельному режимі

У той же час спостерігається залежність реалізації мережевих служб і конкретних додатків від версії протоколу мережевої безпеки. Зниження рівня (по специфікації моделі OSI) підвищує універсальність застосовуваних засобів захисту для будь-яких додатків і протоколів прикладного рівня, однак виникає залежність протоколу захисту від конкретної мережевої технології; компромісним варіантом є протоколи мережевої безпеки IPSec, які функціонують на мережевому рівні. З одного боку, вони «прозорі» для додатків, а з іншого – можуть працювати практично у всіх мережах, оскільки засновані на

широко розповсюдженому протоколі IP.

На сьогодні, протоколи IPSec домінують у більшості із реалізацій віртуальних приватних мереж і реалізовуються як на програмному рівні (наприклад, протоколи реалізовані в операційній системі Windows компанії Microsoft), так і у вигляді програмно-апаратних реалізацій (рішення Cisco, Nokia).

Незважаючи на велике число різних рішень, усі реалізації володіють високою сумісністю один з одним; для контролю цілісності та автентичності пакетів даних у протоколах IPSec застосовуються спеціальні механізми захисту. Їх застосування дозволяє, за рахунок внесення в дані, що передаються спеціально сформованої надмірності (MDC, MAC) ефективно вирішувати задачі захисту пакетів даних від випадкового і зловмисного зміни. Формування кодів контролю цілісності та автентичності пакетів даних засноване на використанні ключових (MAC) та безключових (MDC) функцій гешування. Зазначені механізми застосовуються за замовчуванням у протоколах IPSec з метою забезпечення цілісності та автентичності пакетів даних для усіх реалізацій мереж IPv6.

Протокол SSL (Secure Socket Layer). Протокол SSL розроблено для забезпечення надійного захисту наскрізної передачі даних із використання протоколу TCP.

SSL становить не один протокол, а два рівні протоколів (рис. 11.18).

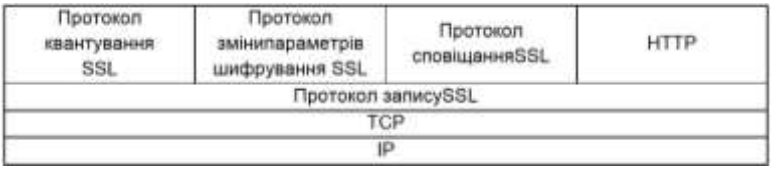

Рисунок 1.18 – Стік протоколів SSL

Протокол SSL пропонує базовий набір засобів захисту, які застосовуються протоколами більш високих рівнів, і забезпечує конфіденційність каналу комунікацій і автентифікацію користувача.

Протокол діалогу SSL має дві основні фази. Перша фаза використовується для встановлення конфіденційного каналу комунікацій. Друга – призначена для автентифікації користувача.

Протокол TLS. Протокол TLS призначений для забезпечення конфіденційності й цілісності даних. Він має два рівні: протокол записів TLS і протокол діалогу TLS.

Протокол записів TLS забезпечує конфіденційність даних з використанням симетричних алгоритмів шифрування DES, RC4 і цілісність даних з використанням геш-функцій SHA-1 або MD5.

Протокол діалогу TLS забезпечує цифровий підпис, заснований на підході RSA або DSS.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Принципи захисту інформації при підключенні до мережі Internet.
2. Захист інформації в ІС за допомогою міжмережевих екранів.
3. Захист інформації за допомогою протоколів TLS, SSL, IPSec.
4. Режими використання мережевих протколів.
5. Схеми проходження IP-пакетів даних.
6. Протоколи безпеки AH і ESP в тунельному та транспортному режимах.
7. Забезпечення конфіденційності, цілісності та автентичності даних під час використання протоколу ESP (IPSec) в IP-мережах.
8. Забезпечення безпеки даних в ІС за допомогою Log-сервера.
9. Забезпечення безпеки даних в ІС за допомогою Proxy-сервера.
10. Забезпечення безпеки даних в інформаційних системах за допомогою демілітаризованої зони.
11. Забезпечення електронної пошти за допомогою антивірусних програм.

Література: [2; 5-11; 14-17].

Тема 12. Заходи щодо захисту інформації

План:

12.1 Методика визначення складу інформації, яку захищають
12.2 Організаційні та інженерно-технічні заходи захисту інформації
12.3 Суб'єкт та об'єкт захисту інформації
12.4 Основні вимоги, які висуваються до системи захисту інформації
12.5 Концептуальні підходи до проектування систем захисту

12.1 Методика визначення складу інформації, яку захищають

Визначення складу інформації, яку необхідно захищати – це перший крок на шляху до побудови системи захисту. Від того, наскільки точно його буде виконано, залежить результат функціонування розроблюваної системи. Загальний підхід полягає у тому, що захисту підлягає вся інформація із обмеженим доступом (ІОД): інформація, яка становить державну таємницю

(секретна інформація); інформація, яка становить комерційну таємницю і визначається власником; частина відкритої інформації. При цьому ІОД повинна захищатися від витоку й втрати, а відкрита – тільки від втрати.

Захист відкритої (публічної) інформації існував завжди та здійснювався шляхом реєстрації її носіїв, обліку їх руху і місцезнаходження. Створювалися безпечні умови зберігання. Відкритість інформації не применшує її цінності, а цінна інформація потребує захисту від втрати. Цей захист не повинен бути спрямованим на обмеження загальнодоступності інформації. Не може бути відмови в доступі до інформації, але доступ повинен здійснюватися із дотриманням вимог відносно її збереження відповідно до вимог обробки та використання.

Інформація – це характеристика взаємодії повідомлення з користувачем.

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, яку було отримано, або створено під час виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених законом України «Про доступ до публічної інформації».

Інформація з обмеженим доступом поділяється на: конфіденційну, таємну та службову.

Конфіденційна інформація – це та, доступ до якої обмежено фізичною або юридичною особою, окрім суб'єктів владних повноважень, та яка може поширюватись у визначеному ними порядку за їх бажанням відповідно до передбачених ними умов.

Таємна інформація – це та інформація, доступ до якої обмежується, розголошення якої може завдати шкоду особі, суспільству, державі. Таємною визначається інформація, яка містить державну, професійну, банківську таємницю, таємницю розслідування та іншу передбачену законом таємницю.

До службової може належати перерахована нижче інформація.

1. Інформація, яка міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані із розробкою напряму діяльності установи або здійсненням контрольних наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень.

2. Інформація, яку зібрано під час оперативно-розшукової та контррозвідувальної діяльності у сфері оборони України, яку не віднесено до

державної таємниці.

Інформаційна безпека – це стан інформації, при якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Складові інформаційної безпеки – це конфіденційність, цілісність, доступність.

Конфіденційність – це властивість інформації, яка не підлягає розголошенню, секретність, суто приватність.

Цілісність – це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Інформація зберігає цілісність, якщо документуються встановлені правила її модифікації та видалення.

Доступність – це властивість інформаційного ресурсу, яка полягає в тому, що користувач або процес, який має відповідні повноваження, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки.

12.2 Організаційні та інженерно-технічні заходи захисту інформації

Організаційні заходи. Організаційні заходи містять у собі створення концепції інформаційної безпеки, а також:

– складання посадових інструкцій для користувачів та обслуговувального персоналу;

– створення правил адміністрування компонентів інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

– розроблення планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

– навчання користувачів правилам інформаційної безпеки.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, режимно-пропускний відділ, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи. Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захисту інформації, який необхідно забезпечити.

Інженерно-технічні заходи, які проводяться для захисту інформаційної інфраструктури організації, можуть охоплювати використання захищених

підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися встановлення в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом. Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

12.3 Суб'єкт та об'єкт захисту інформації

Суб'єкти комплексної системи захисту інформації. До процесу створення комплексної системи захисту інформації (КСЗІ) залучаються наступні сторони:

– організація, для якої здійснюється побудова КСЗІ (Замовник);

– організація, яка здійснює заходи з побудови КСЗІ (Виконавець);

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) (орган контролю);

– організація, яка здійснює державну експертизу КСЗІ (Організатор експертизи);

– організація, у разі необхідності, залучена Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єкти захисту КСЗІ. Захист інформації повинен бути системним, що містить в собі різні взаємопов'язані компоненти. Найважливішим із цих компонентів є об'єкти захисту, бо від їх складу належать і методи, і засоби захисту, і склад захисних заходів.

Інформація є предметом захисту, але захищати її як таку неможливо, оскільки вона не існує сама по собі, а фіксується (відображається) в певних матеріальних об'єктах або пам'яті людей, які виступають в ролі її носіїв і складають основний, базовий об'єкт захисту.

Для запису як секретної, так і несекретної інформації використовуються одні і ті ж носії.

Як правило, носії ІОД охороняються власником цієї інформації.

Носії захищуваної інформації можна класифікувати як: документи; вироби (предмети); речовини і матеріали; електромагнітні, теплові, радіаційні та інші випромінювання; акустичні та інші поля тощо.

Особливим носієм інформації є людина, мозок якої являє виключно складну систему, що зберігає і переробляє інформацію, яка надходить із

навколишнього середовища. Властивість мозку відображати і пізнавати зовнішній світ, накопичувати в пам'яті великі об'єми інформації ставлять людину на особливе місце як носія інформації. Людина має можливість генерувати нову інформацію. І як носій інформації має позитивні та негативні риси.

Позитивні – без згоди суб'єкта-носія захищувана інформація з його пам'яті, як правило, не може бути вилучена. Вона може оцінювати важливість наявної у ннї інформації і відповідно до цього ставитися до неї. Вона може ранжувати споживачів захищуваної інформації, знати, кому і яку інформацію може довірити.

Негативні – вона може помилятися щодо істинності споживача захищуваної інформації або навмисно не зберігати довірену їй інформацію (зрада чи просто поширення).

Серед найбільш поширених видів носіїв конфіденційної інформації можна виділити такі, які перераховано нижче.

1. Паперові носії, в яких інформація фіксується рукописним, машинописним, електронним, типографським та іншими способами в формі тексту, креслення, схеми, формул.

2. Магнітні носії: аудіокасети (аудіоплівки) для магнітофонів і диктофонів; відеокасети (відеоплівки) для відеомагнітофонів та деяких відеокамер; жорсткі (тверді) диски, дискети, магнітні стрічки для ЕОМ. У цих носіях інформація фіксується (наноситься) за допомогою магнітного накопичувача (запису сигналів), який здійснюється магнітним пристроєм, а відображається у вигляді символів. Відтворення (зчитування) інформації здійснюється також магнітним пристроєм за допомогою відновлення сигналів.

3. Магнітооптичні та оптичні носії (лазерні диски, компакт-диски). Запис даних на них виконується лазерним променем (у магнітооптичних і магнітним полем), інформація відображається у вигляді символів, а її зчитування (відтворення) здійснюється за допомогою лазерного променя.

4. Продукція, яка виготовляється (вироби). Ці вироби виконують своє пряме призначення і одночасно є носіями захищуваної інформації. У цьому випадку інформація відображається у вигляді технічних рішень.

5. Технологічні процеси виготовлення продукції, які охоплюють як технологію виробництва продукції, так і застосовувані під час її виготовлення компоненти (засоби виробництва): обладнання, прилади, матеріали, речовини, сировину, паливо тощо. Інформація відображається у вигляді технічних процесів (перша складова) і технічних рішень (друга складова).

6. Фізичні поля, в яких інформація фіксується шляхом зміни їх інтенсивності, кількісних характеристик, відображається у вигляді сигналів, а в електромагнітних полях і у вигляді образів.

Носії ІОД, як об'єкти захисту повинні захищатися, залежно від їх видів, від несанкціонованого доступу, від втрати і від витоку накопиченої інформації у них.

Але, щоб забезпечити захист, необхідно захищати і об'єкти, які є підступом до носіїв, і їх захист виступає у ролі певних рубежів захисту. Чим таких рубежів буде більше, тим складніше їх буде подолати, тим надійніше забезпечиться захист носіїв.

У якості першого рубежа доцільно розглядати прилеглу до установи територію. Деякі підприємства на периметрі встановлюють пропускний пункт. Прилегла територія захищається від несанкціонованого проникнення осіб до будівель підприємства і відходів на виробництво (за їх наявності).

Іншим об'єктом захисту є самі будівлі. Їх захист здійснюється тими ж способами й ставлять ту ж саму мету, що й охорона території. Захист будівель є другим рубежем захисту носіїв.

Наступним об'єктом захисту є приміщення, у яких розташовано сховища носіїв, проводиться обробка носіїв і здійснюється управлінсько-виробнича діяльність із використанням різного роду носіїв інформації. До таких приміщень належать:

– приміщення підрозділів захисту інформації, у яких розташовано сховища носіїв і здійснюється їх обробка (ці приміщення повинні бути захищені від несанкціонованого проникнення);

– приміщення, в яких проводиться робота з носіями інформації або протягом робочого дня, або цілодобово (ці приміщення повинні захищатися під час перебування в них носіїв від несанкціонованого проникнення, від візуального спостереження за носіями, а також, в разі необхідності, від прослуховування конфіденційних розмов, які можуть вестися в них).

Захист здійснюється в приміщеннях співробітниками, які там працюють, різними технічними засобами, в тому числі в неробочий час засобами охоронної сигналізації.

Ще одним об'єктом захисту є безпосередньо сховища носіїв. Сховища захищаються від несанкціонованого доступу до носіїв. Їх захист здійснюється відповідальними зберігачами за допомогою замків, а у позаробочий час вони можуть, окрім замків, захищатися засобами охоронної сигналізації.

Крім того, об'єктами захисту повинні бути:

– засоби відображення, обробки, відтворення і передачі конфіденційної інформації, в тому числі ЕОМ, які повинні захищатися від несанкціонованого підключення, побічних електромагнітних випромінювань, зараження вірусом, електронних закладок, візуального спостереження, виведення з ладу, порушення режиму роботи;

– копіювально-розмножувальна техніка, яка захищається від візуального спостереження і побічних електромагнітних випромінювань під час обробки інформації;

– засоби відео-, звукозаписувальної та відтворювальної техніки, які вимагають захисту від прослуховування, візуального спостереження і побічних електромагнітних випромінювань;

– засоби транспортування носіїв конфіденційної інформації, які підлягають захисту від проникнення сторонніх осіб до носіїв або їх знищення під час транспортування;

– засоби радіо- і кабельного зв'язку, радіомовлення і телебачення, які використовуються для передачі конфіденційної інформації, які повинні захищатися від прослуховування, виведення з ладу, порушення режиму роботи;

– системи забезпечення функціонування підприємства (електро-, водопостачання, кондиціонування тощо), які повинні захищатися від використання їх для виведення з ладу засобів обробки і передачі інформації, прослуховування конфіденційних розмов, візуального спостереження за носіями;

– технічні засоби захисту інформації та контролю за ними, що вимагають захисту від несанкціонованого доступу з метою виведення їх з ладу.

12.4 Основні вимоги, які висуваються до системи захисту інформації

Основні вимоги до комплексної системи захисту інформації. Система захисту інформації повинна забезпечувати виконання автоматизованою системою своїх основних функцій без істотного погіршення характеристик останньої.

Вона повинна бути економічно доцільною, оскільки вартість системи захисту інформації входить у вартість АС.

Захист інформації в АС повинен забезпечуватися на усіх етапах життєвого циклу, за усіх технологічних режимах обробки інформації, у тому числі при

проведенні ремонтних і регламентних робіт.

В систему захисту інформації повинні бути закладені можливості її вдосконалення і розвитку відповідно до умов експлуатації та конфігурації АС.

Відповідно до встановлених правил КСЗІ повинна забезпечувати розмежування доступу до ІОД із відволіканням порушника на помилкову інформацію, тобто мати властивості активного і пасивного захисту.

Під час взаємодії захищеної АС з незахищеними АС система захисту повинна забезпечувати дотримання встановлених правил розмежування доступу.

Система захисту повинна дозволяти проводити облік і розслідування випадків порушення безпеки інформації в АС.

Застосування системи захисту не повинно погіршувати екологічну обстановку, не бути складною для користувача, не викликати психологічної протидії та бажання обійтися без неї.

Завдання комплексної системи захисту інформації. Перелік основних завдань, які повинні вирішуватися КЗСІ:

– управління доступом користувачів до ресурсів АС з метою її захисту від неправомірного, випадкового або навмисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних і апаратних ресурсів з боку сторонніх осіб, а також осіб із числа персоналу організації та користувачів;

– захист даних, які передаються по каналах зв'язку;

– реєстрація, збір, зберігання, оброблення і видача відомостей про усі події, які відбуваються в системі та які стосуються її безпеки;

– контроль роботи користувачів системи з боку адміністрації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль і підтримка цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;

– забезпечення замкнутого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм (у яких можуть міститися шкідливі закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження та розповсюдження комп'ютерних вірусів;

– управління засобами системи захисту.

Основні принципи організації КСЗІ. Захист інформації в АС повинен ґрунтуватися на таких основних принципах:

– системності;

– комплексності;
– безперервності захисту;
– розумної достатності;
– гнучкості управління і застосування;
– відкритості алгоритмів і механізмів захисту;
– простоти застосування захисних заходів і засобів.

Принцип системності. Системний підхід до захисту комп'ютерних систем передбачає необхідність врахування усіх взаємозв'язаних, взаємодійних і змінних в часі елементів, умов та чинників, які є істотно значимі для розуміння і вирішення проблеми забезпечення безпеки.

При створенні системи захисту необхідно враховувати усі слабкі, найбільш вразливі місця системи обробки інформації, а також характер, можливі об'єкти і напрямки атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в розподілені системи і несанкціонованого доступу (НСД) до інформації. Система захисту повинна будуватися з врахуванням не тільки усіх відомих каналів проникнення і НСД до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеці.

Принцип комплексності. У розпорядженні фахівців із комп'ютерної безпеки є широкий спектр заходів, методів і засобів захисту комп'ютерних систем. Комплексне їх використання передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, щояка перекриває усі істотні канали реалізації загроз і не містить слабких місць на стиках окремих її компонентів.

Захист повинен будуватися ешелоновано. Зовнішній захист повинен забезпечуватися фізичними засобами, організаційними та правовими заходами. Однією із найбільш укріплених ліній оборони покликані бути засоби захисту, реалізовані на рівні операційних систем (ОС) в силу того, що ОС – це якраз та частина комп'ютерної системи, яка керує використанням усіх її ресурсів. Прикладний рівень захисту, що враховує особливості предметної області, є внутрішнім рубежем оборони.

Принцип безперервності захисту. Захист інформації – це не разовий захід і навіть не певна сукупність проведених заходів та встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на усіх етапах життєвого циклу АС, починаючи із найперших стадій проектування, а не тільки на етапі її експлуатації.

Розробка системи захисту повинна вестися паралельно із розробкою самої

системи захисту. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і, в підсумку, дозволить створити більш ефективні (як за витратами ресурсів, так і за стійкістю) захищені системи.

Більшості фізичних і технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна та забезпечення правильного зберігання і застосування імен, паролів, ключів шифрування, перевищення повноважень тощо). Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу застосовуваних методів і засобів захисту, для впровадження спеціальних програмних і апаратних «закладок» або інших засобів подолання системи захисту після відновлення її функціонування.

Розумна достатність. Створити на практиці абсолютно неперебороную систему захисту принципово неможливо. При достатній кількості часу і коштів 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 комп'ютерної системи і може створювати відчутні додаткові незручності користувачам. Важливим є правильний вибір достатнього рівня захисту, при якому витрати, ризик і розмір можливого збитку були б прийнятними (задача аналізу ризику).

Гнучкість системи захисту. Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому вжиті заходи та 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 засоби захисту повинні мати певну гнучкість. Особливо важливою ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на систему, яка працює, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом змінюються й властивість гнучкості рятує власників АС від необхідності вживання кардинальних заходів з повної заміни засобів захисту на нові.

Відкритість алгоритмів і механізмів захисту. Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок обмеження доступу до структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання (навіть власникові). Однак це зовсім не означає, що інформація про конкретну систему захисту повинна бути загальнодоступною.

Принцип простоти застосування засобів захисту. Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язаним із знанням спеціальних мов або з виконанням дій, які вимагають значних додаткових трудовитрат при звичайній роботі законних користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (введення декількох паролів, імен тощо).

12.5 Концептуальні підходи до проектування систем захисту

На даний час можливо виділити три концептуальні підходи до проектування систем захисту.

Підхід перший – «від продукту». Цього підходу дотримуються, як правило, компанії-виробники систем захисту інформації, які мають у своєму складі проектну групу. Фактично, в таких компаніях інтеграція виросла із просто впроваджувального напрямку в той момент, коли замовник попросив не просто продукт, а проект. Таким чином, вся технологія проектування орієнтована на те, щоб продукт, вироблений компанією, був центральним незалежно від розв'язуваної задачі. Даний підхід не завжди повністю обґрунтований, особливо в умовах агресивного маркетингу і позиціонування продукту як «панацеї» від більшості загроз безпеки.

Однак у разі, коли замовник має достатню кваліфікацію, щоб широко дивитися на проблему захисту інформації в цілому і уникати однобоких рішень, реалізуються проекти високої якості, що зрозуміло, адже ніхто, крім виробника, не знає продукту краще. Але в цьому випадку необхідно або наявність власних висококласних фахівців, системних архітекторів, або залучення зовнішніх консалтингових компаній.

Другий підхід – компанія виступає постачальником рішень у сфері захисту інформації. Розуміючи відсутність єдиного продукту, який захищає від усіх загроз, компанія пропонує комплексне вирішення проблеми. Воно складається із комбінації декількох технологій захисту, наприклад, міжмережевих екранів для захисту від атак з Інтернету, VPN – для закриття каналів зв'язку тощо.

Формально схема виглядає таким чином: зараз існують чотири основні технології захисту – міжмережеве екранування, VPN, криптографічний захист, активний аудит. Кожна технологія має по три-чотири продукта, які дійсно працюють. Тобто, чотири технології по чотири продукти утворюють 16 рішень, із яких може будуватися система безпеки. Тоді завдання архітектора системи захисту зводиться до того, щоб знайти, куди прилаштувати кожне рішення.

Виникає спокуса починати будувати систему, відштовхуючись не від потреб замовника, а від наявних засобів захисту.

На даний час існує великий неосвоєний ринок середніх і дрібних компаній, для яких занадто дорого купувати серйозні консалтингові послуги компаній-інтеграторів. Таким компаніям як раз і потрібен деякий набір продуктів і рішень, які могли б просто об'єднуватися в систему, надаючи їй необхідну функціональність.

Існує ще й третій підхід – найскладніший і такий, який досить рідко зустрічається на нашому ринку. Яка стандартна схема продажу певного продукту або системи? Постачальник приходить до замовника, вивчає його проблему і пропонує те чи інше рішення, продукт або варіанти рішення, або замовник організує тендер, отримує декілька пропозицій. І в тому, і в іншому випадку замовник самостійно приймає рішення про те, яку систему, технологію впроваджувати. Тобто, відповідальність за прийняття рішень щодо захисту інформації покладається на замовника, який, взагалі кажучи, не є експертом в галузі захисту інформації. Найскладніше завдання, яке може і повинно стояти перед компанією-інтегратором, – це прийняти на себе відповідальність за вибір стратегії забезпечення безпеки організації, розвиток системи, її адекватність технологіям, які розвиваються. Системний інтегратор повинен реалізовувати єдину комплексну політику, як технічну, так і організаційну, проводячи її на всіх рівнях організації-замовника.

Перед виробленням рішення з інформаційної безпеки інтегратор повинен провести всебічне глибоке обстеження не просто інформаційної системи замовника, а всього «інформаційного життя» установи. Обстеження має здійснюватись на трьох рівнях:

– на рівні бізнес-процесів, який виявляє документальні потоки, типи оброблюваної інформації, рівні її конфіденційності;

– на інфраструктурному рівні – для виявлення вразливих місць серверного парку, мережевого обладнання;

– на рівні додатків, на якому виявляються уразливості в програмному забезпеченні, помилки в налаштуваннях механізмів розмежування доступу тощо.

На основі отриманих даних формують концептуальне рішення щодо захисту інформації, яке складається з комплексу організаційних, процедурних і програмно-апаратних засобів захисту, а потім, чітко обґрунтовуючи вибір, пропонують впровадження тих або інших технологій захисту. При цьому враховують, що підсистема інформаційної безпеки є підтримувальною системою відповідно до всієї інформаційної системи організації. Вона не повинна

відігравати домінуючу роль у розвитку організації та її інформаційної системи. Тобто, система інформаційної безпеки повинна захищати інформацію, яка забезпечує бізнес-завдання організації.

Таким чином, будь-яка система інформаційної безпеки, що захищає велику організацію із розподіленою інформаційною системою, або система, яка являє собою один міжмережевий екран, повинна бути розумно достатньою відносно організації, вона не повинна заважати роботі працівників.

Вибір рівня захисту повинен бути адекватним, при цьому правильним має бути і вибір технологій та засобів захисту.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Яким чином необхідно визначати склад інформації, яку необхідно захищати?
2. Інформація з обмеженим доступом.
3. Конфіденційність, цілісність та доступність інформації.
4. Організаційні заходи в концепції інформаційної безпеки.
5. Інженерно-технічні заходи в концепції інформаційної безпеки.
6. Комплексна система захисту інформації: суб'єкти та об'єкти захисту.
7. Класифікація носіїв захищуваної інформації.
8. Позитивні та негативні властивості носія інформації.
9. Види носіїв конфіденційної інформації.
10. Рубежі захисту інформації з обмеженим доступом.
11. Об'єкти захисту.
12. Які вимоги висуваються до системи комплексного захисту інформації?
13. Основні завдання системи комплексного захисту інформації.
14. Принципи організації системи комплексного захисту інформації.
15. Суть принципу відкритості алгоритмів і механізмів захисту?
16. Концептуальні підходи до проектування систем захисту?

Література: [1-17].

Тема 13. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності

План:

13.1 Етапи технічного захисту інформації

13.2 Організація розроблення системи захисту інформації

13.3 Реалізація організаційних заходів захисту

13.4 Реалізація первинних та основних технічних заходів захисту

13.1 Етапи технічного захисту інформації

Технічний захист інформації здійснюється поетапно:

– 1-ий етап – визначення й аналіз загроз;
– 2-ий етап – розроблення системи захисту інформації;
– 3-ий етап – реалізація плану захисту інформації;
– 4-ий етап – контроль функціонування та керування системою ЗІ.

Сукупність дій, які здійснюються об'єктом для досягнення певної мети, реалізується у вигляді результатів, які мають значення для самого об'єкта. Якщо мета операції або сукупності цілеспрямованих дій досягнута, то безпеку операції, а отже, інформації, яка циркулює в системі, забезпечено.

Проблема дослідження критичних ситуацій та чинників, які можуть становити певну небезпеку для інформації, а також пошуку та обґрунтування комплексу заходів і засобів з їх усунення або зниження характеризується наступними особливостями:

– великою кількістю чинників небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;

– необхідністю виявлення і вивчення повного спектра можливих заходів і засобів парирування небезпечних факторів з метою забезпечення безпеки.

Як бачимо, загроза інформації обумовлена цілком певними чинниками, сукупністю явищ та умов, які можуть скластися в конкретній ситуації.

Відносно інформаційної системи усю сукупність загроз доцільно розбити на дві групи: зовнішні і внутрішні, кожна з яких, в свою чергу, ділиться на умисні й випадкові загрози, які можуть бути явними і прихованими.

Виявлення та аналіз загроз захисту є відповідальним етапом при побудові системи захисту інформації. Найбільш часто, при цьому, вживають термін «загроза безпеки інформації». Але безпека інформації – це стан захищеності інформації від впливів, які порушують її цілісність. Отже, безпека інформації означає, що інформація знаходиться в такому захищеному вигляді, який здатний протистояти будь-яким дестабілізувальним впливам.

Будь-яка загроза не зводиться до чогось однозначного, вона складається із певних взаємопов'язаних компонентів, кожен з яких сам по собі не створює загрозу, але є її невід'ємною частиною, загроза виникає лише при сукупній їх взаємодії.

Загрози захисту інформації пов'язані з її вразливістю, тобто нездатністю інформації самостійно протистояти таким дестабілізувальним впливам, що порушують її статус. Реалізація загроз призводить, залежно від їх характеру, до однієї або кількох форм прояву уразливості інформації. При цьому, кожній із

форм прояву уразливості (або декільком з них) притаманні певні, що стосуються тільки її, загрози з набором відповідних компонентів. Структура конкретної загрози зумовлює конкретну форму. Однак повинна існувати і загальна, так би мовити, типова структура загроз, яка складає основу конкретних загроз. Ця загальна структура повинна базуватися на певних ознаках, характерних для загрози захисту інформації.

Визначальною ознакою загрози є її спрямованість, результат, до якого може призвести дестабілізувальний вплив на інформацію. Цим результатом у всіх випадках реалізацій загрози є порушення статусу інформації. Таким чином, загроза інформації – це сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації. На практиці, до явищ сутнісних проявів загрози прийнято відносити:

– джерела дестабілізувального впливу на інформацію (від кого або від чого виходить дестабілізувальний вплив);

– види дестабілізувального впливу на інформацію (яким чином та за якими напрямками відбувається дестабілізувальний вплив);

– способи дестабілізувального впливу на інформацію (якими прийомами, діями здійснюються (реалізуються) види дестабілізувального впливу).

До чинників, окрім причин та обставин, необхідно віднести також й наявність каналів і методів несанкціонованого доступу до конфіденційної інформації для впливу на інформацію з боку осіб, які не мають до неї дозволеного доступу.

Доцільно звернути увагу на те, що джерела, самі по собі, не є загрозою, якщо від них не виходить той або інший вплив. До джерел дестабілізувального впливу на інформацію належать:

– люди;

– технічні засоби відображення (фіксації), зберігання, обробки, відтворення, передачі інформації, засоби зв’язку;

– системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації;

– технологічні процеси окремих категорій промислових об’єктів;

– природні явища.

Одним із найпоширеніших, різноманітних та найнебезпечніших джерел дестабілізувального впливу на захищувану інформацію є людина. За співвідношенням до видів та способів дестабілізувального впливу на інформацію категорії працівників поділяють на дві групи: ті які володіють доступом до носіїв захищуваної інформації, технічних засобів її відображення,

зберігання, обробки, відтворення, передачі і систем забезпечення їх функціонування, та ті які такого доступу не мають.

Технічні засоби відображення, зберігання, обробки, відтворення, передачі інформації і засоби зв'язку є другим за значенням джерелом дестабілізувального впливу на захищувану інформацію. До даного джерела належать:

– електронно-обчислювальна техніка;

– електричні та автоматичні друкарські машинки і копіювальнорозмножувальна техніка;

– засоби відео- та звукозаписувальної і відтворювальної техніки;

– засоби телефонного, телеграфного, факсимільного, гучномовного передавання інформації;

– засоби радіомовлення і телебачення;

– засоби радіо- і кабельного зв'язку.

Третє джерело дестабілізувального впливу на інформацію охоплює системи електропостачання, водопостачання, теплопостачання, кондиціонування.

До четвертого джерела відносять технологічні процеси об'єктів ядерної енергетики, хімічної промисловості, радіоелектроніки, а також об'єктів із виготовлення деяких видів озброєння і військової техніки, які змінюють природну структуру навколишнього середовища.

П'яте джерело – природні явища (стихійні лиха і атмосферні явища).

Методика виявлення способів впливу на інформацію. У залежності від джерела та виду впливу на захищувану інформацію, на практиці, прийнято розрізняти безпосереднє, опосередковане або інше джерело впливу.

Способами безпосереднього впливу на носії захищуваної інформації можуть бути:

– фізичне руйнування носія (поломка, руйнування тощо);

– створення аварійних ситуацій для носіїв (вибух, затоплення тощо);

– видалення інформації з носіїв;

– створення штучних магнітних полів для розмагнічування носіїв;

– внесення фальсифікованої інформації у носії.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву вразливості інформації: знищення, спотворення і блокування.

До безпосереднього впливу на носії захищуваної інформації можна віднести й ненавмисне залишення їх в неохоронній зоні, найчастіше в громадському транспорті, магазині, що призводить до втрати носіїв.

Несанкціоноване розповсюдження інформації з обмеженим доступом (ІОД) здійснюється шляхом:

– словесної передачі (повідомлення) інформації;
– передачі копій (знімків) носіїв інформації;
– показу носіїв інформації;
– введення інформації в обчислювальні мережі;
– опублікування інформації в пресі;
– використання інформації у відкритих публічних виступах, в тому числі по радіо, телебаченню.

До розголошення може призвести і втрата носіїв інформації. Цей вид дестабілізувального впливу призводить до розголошення ІОД.

У свою чергу, до способів виведення з ладу технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації та засобів зв'язку можна віднести:

– неправильний монтаж засобів;
– поломку (руйнування) засобів, в тому числі розрив (пошкодження) кабельних ліній зв'язку;
– створення аварійних ситуацій для засобів (підпал, штучне затоплення, вибух та ін.);
– відключення засобів від систем;
– виведення з ладу або порушення режиму роботи систем забезпечення функціонування засобів;
– вмонтування в ЕОМ радіо- і програмних закладних пристроїв.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, спотворення і блокування.

Способами порушення режиму роботи технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації, засобів зв'язку і технології обробки інформації можуть бути:

– пошкодження окремих елементів засобів;
– порушення правил експлуатації засобів;
– внесення змін до порядку обробки інформації;
– зараження програм обробки інформації шкідливими програмами;
– видача неправильних програмних команд;
– перевищення розрахункового числа запитів;
– створення завад у радіоефірі за допомогою додаткового звукового або шумового фону, зміни (накладення) частот передачі інформації;
– передача хибних сигналів;
– порушення (зміна) режиму роботи систем забезпечення функціонування засобів.

Даний вид дестабілізувального впливу також призводить до знищення, перекручення і блокування інформації.

До способів виведення з ладу і порушення режиму роботи систем забезпечення, функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації слід віднести:

– неправильний монтаж систем;

– поломку (руйнування) систем або їх елементів;

– створення аварійних ситуацій для систем (підпал, штучне затоплення, вибух тощо);

– відключення систем від джерел живлення;

– порушення правил експлуатації систем.

Цей вид дестабілізувального впливу призводить до тих же результатів, що і два попередні види.

До видів дестабілізувального впливу на захищувану інформацію з боку іншого джерела впливу – технічних засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв'язку – відносять:

– виведення засобів з ладу;

– збої в роботі засобів;

– створення електромагнітних випромінювань.

Вихід засобів з ладу, що призводить до неможливості виконання операцій, може відбуватися шляхом:

– технічної поломки, аварії (без втручання людей);

– загоряння, затоплення (без втручання людей);

– виходу з ладу систем забезпечення функціонування засобів;

– впливу природних явищ;

– впливу зміненої структури навколишнього магнітного поля;

– зараження програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– руйнування або пошкодження носія інформації, в тому числі розмагнічування магнітного шару диска (стрічки) через осипання магнітного порошку.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, перекручення, блокування.

Збої в роботі засобів, що призводять до неправильного виконання операцій (помилок), можуть відбуватися в зв'язку з:

– зараженням програм обробки інформації шкідливими програмами (шляхом розмноження останніх або з заражених дискет);

– виникненням технічних несправностей елементів засобів;

– впливом природних явищ;

– впливом навколишнього магнітного поля;

– частковим розмагнічуванням магнітного шару диска (стрічки) через осипання магнітного порошку; – порушенням режиму функціонування засобів.

Даний вид дестабілізувального впливу призводить до реалізації чотирьох форм прояву уразливості інформації: знищення, перекручення, блокування, розголошення (приклад останньої – телефонне з'єднання не з тим абонентом, який набирався, або чутність розмови інших осіб через несправність в ланцюгах комунікації телефонної станції).

Електромагнітні випромінювання, в тому числі побічні, які утворюються під час експлуатації засобів, призводять до розкрадання інформації. Це ще одне джерело дестабілізувального впливу на інформацію – системи забезпечення функціонування технічних засобів відображення, зберігання, обробки, відтворення і передачі інформації – якому притаманні такі види впливу:вихід систем з ладу та збої в роботі систем. Вихід систем з ладу може відбуватися шляхом:

– поломки, аварії (без втручання людей) або загоряння;затоплення (без втручання людей);

– виходу з ладу джерел живлення;

– впливу природних явищ.

Цей вид дестабілізувального впливу призводить до реалізації трьох форм прояву уразливості інформації: знищення, блокування, викривлення.

Збої в роботі систем можуть здійснюватися за допомогою:

– появи технічних несправностей елементів систем;

– впливу природних явищ;

– порушення режиму роботи джерел живлення.

Результатом дестабілізувального впливу також є знищення, блокування, спотворення інформації.

Видом дестабілізувального впливу на інформацію з боку технологічних процесів окремих промислових об'єктів є зміна структури навколишнього середовища. Це вплив здійснюється шляхом:

– зміни природного радіаційного фону навколишнього середовища, що відбувається при функціонуванні об'єктів ядерної енергетики;

– зміни хімічного складу навколишнього середовища, що відбувається при функціонуванні об'єктів хімічної промисловості;

– зміни локальної структури магнітного поля, що відбувається внаслідок

діяльності об’єктів радіоелектроніки і з виготовлення деяких видів озброєння і військової техніки.

Цей вид дестабілізувального впливу в кінцевому підсумку призводить до розкрадання ІОД.

Останнє джерело дестабілізувального впливу на інформацію – природні явища, що охоплюють стихійні лиха і атмосферні явища (коливання). До стихійних лих і одночасно видів впливу слід віднести: землетруси, повені, шторми, зсуви, лавини, виверження вулканів; до атмосферних явищ: грозу, дощ, сніг, перепади температури і вологості повітря, магнітні бурі.

Способами впливу з боку і стихійних лих, і атмосферних явищ можуть бути руйнування (поломки), землетруси, загоряння носіїв інформації засобів відображення, зберігання, обробки, відтворення, передачі інформації і засобів зв’язку, систем забезпечення функціонування цих засобів, порушення режиму роботи засобів і систем, а також технології обробки інформації, створення паразитних наведень (грозові розряди).

Ці види впливу призводять до п’яти форм прояву уразливості інформації: втрати, знищення, перекручення, блокування і розкрадання.

Під час розгляду ознак і складових загрози захищуваній інформації видно, що в основі будь-якого дестабілізувального впливу лежать певні причини, спонукальні мотиви, які зумовлюють появу того чи іншого виду і способу впливу. Разом з тим і причини мають під собою підстави – обставини або передумови, які викликають ці чинники, сприяють їхній появі. Однак наявність джерел, видів, способів, причин і обставин (передумов) дестабілізувального впливу на інформацію є потенційно існуючою небезпекою, яка може бути реалізована тільки за наявності певних умов для цього.

13.2 Організація розроблення системи захисту інформації

Розроблення плану захисту інформації. Розроблення плану ТЗІ має містити організаційні, первинні технічні та основні технічні заходи захисту ІОД із обов’язковим визначенням зон безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності (ІД) із врахуванням норм та вимог ТЗІ для всіх періодів життєвого циклу ІОД. Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ. Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ. При цьому, заходи захисту інформації повинні:

– бути відповідними загрозам;

– бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;

– забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень захисту інформації визначається системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог ТЗІ. При цьому, мінімально необхідний рівень захисту інформації необхідо забезпечувати обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі. Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії до безлічі загроз.

Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) регламентується нормативними документами системи ТЗІ.

Реалізація плану захисту інформації. Наступним етапом ТЗІ є реалізація організаційних, первиннних та основних технічних заходи захисту ІОД, установлення необхідних зони безпеки інформації, проведення атестації технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів та систем.

Засоби ТЗІ можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, які володіють, користуються і розпоряджаються ІОД самостійно або за рекомендаціями спеціалістів з ТЗІ відповідно до нормативних документів системи ТЗІ.

Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів

забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, які мають ліцензію на право проведення цих робіт, видану Державною службою спеціального зв'язку та захисту інформації України.

Організація проведення обстеження об'єктів інформаційної діяльності. Метою обстеження об'єктів інформаційної діяльності є вивчення їх ІД, визначення об'єктів захисту – ІОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

Обстеження, зазвичай, проводиться комісією, склад якої визначається відповідно за ТЗІ особою і затверджується наказом керівника підприємства. У ході обстеження необхідно:

– провести аналіз умов функціонування ОІД підприємства, їх розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

– дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

– вивчити схеми засобів і систем життєзабезпечення ОІД (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;

– дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі – оброблення) інформації і провести необхідні вимірювання;

– визначити наявність та технічний стан засобів забезпечення ТЗІ;

– перевірити наявність на ОІД нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

– виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

– визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

– визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна містити:

– генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

– схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІОД;

– оцінку шкоди, яка передбачається від реалізації загроз.

Організація розроблення системи захисту інформації. На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації. ТЗ повинно мати такі основні розділи:

– вимоги до системи захисту інформації;

– вимоги до складу проектної та експлуатаційної документації;

– етапи виконання робіт;

– порядок внесення змін і доповнень до розділів ТЗ;

– вимоги до порядку проведення випробування системи захисту.

Основою функціонування системи захисту інформації є план ТЗІ, який повинен містити наступні документи:

– перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;

– інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;

– інструкції, що встановлюють обов'зки, права та відповідальність персоналу;

– календарний план ТЗІ.

ТЗ і план ТЗІ розробляють спеціалісти у цй сфері діяльності, узгоджують із зацікавленими підрозділами (організаціями), а затверджує їх керівник підприємства.

13.3 Реалізація організаційних заходів захисту

Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ. Під час розроблення та реалізації організаційних заходів необхідно:

– визначити окремі задачі захисту ІзОД;

– обґрунтувати структуру і технологію функціонування системи захисту інформації;

– розробити і впровадити правила реалізації заходів ТЗІ;

– визначити і встановити права та обов'язки підрозділів і осіб, які беруть участь в обробленні ІзОД;

– придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними ОІД підприємства;

– встановити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

– встановити порядок контролю функціонування системи захисту інформації та її якісних характеристик;

– визначити зони безпеки інформації;

– установити порядок проведення атестації системи захисту інформації, її елементів і розробити програми атестаційного випробування;

– забезпечити керування системою захисту інформації.

Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

– вивчати й аналізувати технологію проходження ІОД у процесі ІД;

– оцінювати схильність ІОД до впливу загроз у конкретний момент часу;

– оцінювати очікувану ефективність застосування засобів ТЗІ;

– визначати додаткову потребу в засобах забезпечення ТЗІ;

– здійснювати збір, оброблення та реєстрацію даних, які стосуються ТЗІ;

– розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

13.4 Реалізація первинних та основних технічних заходів захисту

Реалізація первинних технічних заходів захисту. Під час реалізації первинних технічних заходів необхідно, перш за все, забезпечити:

– блокування каналів витоку інформації;

– блокування несанкціонованого доступу до інформації або її носіїв;

– перевірку справності та працездатності технічних засобів забезпечення інформаційної діяльності.

Блокування каналів витоку інформації може здійснюватися шляхом:

– демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано із життєзабезпеченням ОІД та обробленням ІОД;

– видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІОД;

– тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;

– застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

Блокування несанкціонованого доступу до інформації або її носіїв може здійснюватися за рахунок:

– створення умов роботи в межах установленого регламенту;

– унеможливлення використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно проводити відповідно до експлуатаційної документації. Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації та підлягають негайній заміні (демонтажу).

Реалізація основних технічних заходів захисту. Під час реалізації основних технічних заходів захисту необхідно:

– встановити засоби виявлення та індикації загроз і перевірити їх працездатність;

– встановити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їх працездатність;

– застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє тестування і тестування на відповідність вимогам захищеності;

– застосувати спеціальні інженерно-технічні споруди, засоби (системи).

Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації. Фрагментарний захист забезпечує протидію певній загрозі. Комплексний захист забезпечує одночасну протидію безлічі загроз.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІОД про витік інформації чи порушення її цілісності. Засоби ТЗІ застосовують автономно або спільно із технічними засобами забезпечення ІД для пасивного або активного приховування ІОД. Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани. Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

Програмні засоби застосовуються для забезпечення:

– ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

– розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

– цілісності інформації та конфігурації автоматизованих систем;

– реєстрації та обліку дій користувачів;

– маскування оброблюваної інформації;

– реагування (сигналізація, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації. До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо. Розміщення, монтаж та прокладання спеціальних інженернотехнічних засобів і систем, серед них систем заземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять відповідно до експлуатаційної документації.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Етапи ТЗІ
2. Визначення та аналіз загроз.
3. Система захисту інформації.
4. Методика виявлення способів впливу на інформацію.
5. План захисту інформації: розроблення та його реалізація.
6. Джерела дестабілізувального впливу на інформацію.
7. Первинні та основні технічні заходи захисту.
8. Безпосередній та опосередкований вплив на інформацію.
9. Форми прояву вразливості інформації: їх суть та від чого вони залежать.
10. Несанкціонаоване розповсюдження інформації з обмеженим доступом.
11. Види дестабілізувального впливу на захищувану інформацію з боку іншого джерела впливу.
12. Збій в роботі системи ТЗІ та вихід її з ладу.
13. Природні явища, як джерело дестабілізувального впливу на інформацію.

Література: [2; 5-11; 14-17].

ЛІТЕРАТУРА

1. Вакалюк Т. А. Захист інформації в комп'ютерних системах. URL: http://eprints.zu.edu.ua/9650/1/1.pdf (дата звернення: 20.08.2024).
2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Гапак О. М. Криптоаналіз. Криптографічні протоколи : навч. посіб. Ужгород : Вид-во ПП «АУТДОР-ШАРК», 2021.
4. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах : підруч. Ужгород : ДВНЗ «УжНУ», 2021. 184 с.
5. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
6. Гуз А. М. Організація захисту інформації з обмеженим доступом. URL: http://za.inf.ua/bo/oziod18.pdf (дата звернення: 10.07.2024).
7. Заплотинський Б. А. Основи інформаційної безпеки. URL: http://surl.li/pfkpnk (дата звернення: 10.07.2024).
8. Інформаційна безпека / за ред. Ю. Я. Бобала та І. В. Горбатого. URL: http://surl.li/iglfxk (дата звернення: 10.07.2024).
9. Інформаційна безпека : підруч. / за ред. В. Остроухова. К. : Вид-во Ліра-К, 2021. 412 с.
10. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / за ред. О. А. Смірнов. Кропивницький : Видавець Лисенко В. Ф., 2020. 295 с.
11. Кавун С. В. Носов В. В. Манжай О. В. Інформаційна безпека : навч. посіб. URL: http://surl.li/ikprgx (дата звернення: 10.07.2024).
12. Комплексні системи захисту інформації. URL: http://surl.li/yptezr (дата звернення: 10.07.2024).
13. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO : навч. посіб. Львів : Вид-во Львівська політехніка, 2021. 232 с.
14. Лісовська Ю. Кібербезпека. Ризики та заходи. URL: http://surl.li/hrqcoh (дата звернення: 10.07.2024).
15. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека : сучасні технології захисту : навч. посіб. Львів : «Новий Світ-2000», 2020. 678 с.
16. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf (дата звернення: 10.07.2024).
17. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління. URL: http://surl.li/znnide (дата звернення: 10.07.2024).

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Апаратні та програмні засоби захисту інформації: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 252 с.

Комп'ютерний набір та верстка: О. Л. Кайдик.

Редактор: в авторській редакції.

Підп. до друку «__» _____ 2025 р.
Формат 60x84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 16,0. Обл. – вид. арк. 14,74.
Тираж _50_ прим. Зам. _____.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75