МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Карачка А.Ф.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Текст лекцій

Тернопіль, ТНЕУ, 2017

ТЕМА 1. ВСТУП В ДИСЦИПЛІНУ «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

1.1. Інформація як об’єкт захисту.
1.2. Характеристика загроз безпеці інформації.
1.3. Мета і завдання курсу. Місце дисципліни серед інших дисциплін.
1.4. Література.

1.1. Інформація як об’єкт захисту

1.2. Характеристика загроз безпеці інформації

«Концепція технічного захисту інформації в Україні» [ ] визначає такі 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.

Мотивація цих джерел може бути зовсім різною: від повної її відсутності у стихійних лих до економічних та політичних переваг (таблиця 1.1).

Таблиця 1.1 - 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
Окремі фізичні особи	Самоствердження, отримання економічних переваг і винагород
Навмисні та ненавмисні дії персоналу	Помилки персоналу,низька кваліфікація працівників; образа, зрада, промушення
стихійні лиха та техногенні катастрофи	Відсутність мотивації

На основі поданої класифікації джерел можна скласти одну із можливих класифікацій загроз для інформації:

- наслідки стихійних лих і техногенних катастроф;
- відмови обладнання;
- наслідки помилок проектування системи захисту;
- наслідки помилок персоналу;
- навмисні дії порушників.

У теорії захисту інформації доведено, що якщо система захисту побудована

з урахуванням усіх сучасних методів та засобів захисту, а підприємство має ретельно підібраний та навчений персонал, який не допускає помилок, то навмисні дії порушників у такій системі неможливі. Однак насправді це не зовсім правильно. З часом система захисту застаріває, персонал змінюється та втрачає пильність, зловмисники знаходять нові способи атак та методи подолання захисту, невідомі на час розробки системи захисту. Тому маючи обґрунтовані надії на стійкість системи захисту інформації, краще, все ж таки, пам'ятати основне правило захисту інформації: жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника. Це правило вироблено роками досвіду спеціалістів захисту інформації і має універсальний характер. Воно не залежить від рівня системи захисту, сумлінності користувачів та адміністраторів, апаратного та програмного забезпечення. Воно стверджує, що проблема полягає не в тому, чи «зламають» зловмисники систему захисту, а в тому, коли це відбудеться. І завдання захисту інформації полягає в тому, щоб злам системи відбувся якомога пізніше. Про це говорить і мета захисту інформації, визначена в «Концепції технічного захисту інформації»: «метою захисту інформації є 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».

1.3. Мета і завдання курсу. Місце дисципліни серед інших дисциплін

1.4. Література

ОСНОВНА ЛІТЕРАТУРА

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах/ А. О. Антонюк. – К.: КМ Академія, 2006. – 244 с.

2. Белкин П. Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных/ П. Ю. Белкин, О. О. Михальський, А. С. Першаков. - М.: Радио и связь, 1999. - 168 с.

3. Вербіцький О.В. Вступ до криптології/ О. В. Вербіцький. – Львів: Вид-во НТЛ, 2008. - 248 с.

4. Герасименко В. А.Основы защиты информации/ В. А. Герасименко. - М.: Инкомбук, 1997. - 537 с.

5. Гундарь К. Ю. Защита информации в компьютерных системах/ К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К.: Корнійчук, 2008. – 152 с.

6. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты/ В. В. Домарев. - К.: ООО ТИД ДС, 2001. - 688 с.

7. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998.

8. Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.

9. Закон України «Про захист інформації в інформаційно-телекомунікаційних систе-мах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.

10. Закон України «Про інформацію». – К.:Відомості Верховної Ради України, 1992. - N 48. - Ст.650 .

11. Закон України «Про електронний цифровий підпис». – К.:Відомості Верховної Ради України, 2003. - N 36. - Ст.276 .

12. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. – 68 с.

13. Медведовский И. Д. Атака на Internet/ И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. - М.: ДМК, 1999. - 336 с.

14. Петров А. А. Компьютерная безопасность. Криптографические методы защиты/ А. А. Петров. - М.: ДМК, 2000. - 448 с.

ДОДАТКОВА ЛІТЕРАТУРА

15. Баричев С. Г. Основы современной криптографии/ С. Г. Баричев, Р. Е. Серов. – М.: Радио и связь, 2005. – 152 с.

16. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В. Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.

17. Хорошко В. А. Методы и средства защиты информации/В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 501 с.

18. Фаль О. М. Криптографія: основні ідеї та застосування/ О. М. Фаль. – К,: Вид-во НТТУ КПІ, 2004.

19. Ярочкин В. И. Безопасность информационных систем/ В. И. Ярочкин. – М.: Ось-89, 1996. – 320 с.

ТЕМА 2. ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Основні означення та поняття теорії захисту інформації.
2.2. Інформаційна безпека комп'ютерів і комп'ютерних систем.
2.3. Вразливість комп'ютерів і комп'ютерних систем.

2.1. Основні положення та поняття теорії захисту інформації

Щоб в повній мірі задовільнити потреби сучасного суспільства, виникла необхідність інформаційного забезпечення всіх сфер діяльності людини і, зокрема, надійного захисту інформації. Особливої гостроти дана проблема набуває у зв'язку з масовою комп'ютеризацією, об'єднанням комп'ютерів у комп'ютерні мережі та використання Internet.

Інформація – абстрактне поняття, що має різні значення залежно від контексту. Походить від латинського слова «informatio», яке має декілька значень:

- роз'яснення;
- виклад фактів, подій;
- тлумачення;
- представлення, поняття;
- ознайомлення, просвіта.

Ясенєв В.Н. дає більш розгорнуте тлумачення інформації, на його погляд інформація це:

- загальнонаукове поняття, яке включає у себе обмін відомостями між людьми;

- з точки зору прийняття рішень інформацією є дані, які впливають на поведінку системи і використовуються у процесі прийняття рішень або у зв'язку із здійсненням тих або інших дій;

- відомості (відображення) про подію або стан реальної дійсності, що дозволяють приймати рішення, які ведуть до досягнення мети наочної діяльності.

У кібернетиці інформація трактується зазвичай як міра усунення невизначеності знання у одержувача. Іншими словами, інформацією є не будь-яке повідомлення, а лише таке, яке містить невідомі раніше його одержувачеві факти.

У законі України «Про інформацію» наведене таке тлумачення поняття інформація – <u>будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді</u> [7. Розділ 1, стаття 1].

Отже можна визначити інформацію як нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні. Іншими словами, інформація – це нові знання, які отримує суб'єкт у результаті сприйняття і опрацювання певних відомостей.

Інформацію розрізняють і за галузями знань: технічна, економічна, біологічна та інші.

Найважливішими, з практичної точки зору, властивостями інформації є

<u>Цінність інформації</u> – визначається забезпеченням можливості досягнення мети, поставленої перед отримувачем інформації.

Достовірність – відповідність отриманої інформації об'єктивній реальності навколишнього світу.

Актуальність – це міра відповідності цінності та достовірності інформації поточному часу (певному часовому періоду).

Часові властивості визначають здатність даних передавати динаміку зміни ситуації (динамічність).

Оперативність – властивість даних, яка полягає в тому, що час їхнього збору та переробки відповідає динаміці зміни ситуації;

Ідентичність – властивість даних відповідати стану об'єкту.

Для людини інформація поділяється на види залежно від типу рецепторів, що сприймають її.

Візуальна – сприймається органами зору.

Аудіальна – сприймається органами слуху.

Тактильна – сприймається тактильними рецепторами.

Нюхова – сприймається нюховими рецепторами.

Смакова – сприймається смаковими рецепторами

За формою подання інформація поділяється на такі види:

Текстова – що передається у вигляді символів, призначених позначати лексеми мови;

Числова – у вигляді цифр і знаків, що позначають математичні дії;

Графічна – у вигляді зображень, подій, предметів, графіків;

Звукова – усна або у вигляді запису передачі лексем мови аудіальним шляхом.

За призначенням інформацію також можна поділити на такі види:

Масова – містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму.

Спеціальна – містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній масі соціуму, але необхідні і зрозумілі в рамках вузької соціальної групи, де використовується дана інформація

Особиста – набір відомостей про яку-небудь особистість, що визначає соціальний стан і типи соціальних взаємодій всередині популяції.

У законодавстві Україна виділяють інформацію з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежене встановленими правовими нормами та (або) правилами[2].

Інформація таємна (secret information) – інформація з обмеженим доступом, що містить відомості, які становлять державну та іншу передбачену законом таємницю і розголошення яких завдає шкоди особі, суспільству та державі.

Інформація конфіденційна – інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави, і порядок доступу до якої встановлюється ними.

Конфіденційність інформації – властивість інформації, яка полягає в тому,

що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Російський автор В.Н. Ясенєв дає більш цікаве тлумачення поняття «конфіденційність», а саме конфіденційність комп'ютерної інформації, з його точки зору це властивість інформації бути відомою лише допущеним та пройшовшим перевірку суб'єктам системи (користувачам, програмам, процесам та ін.).

Отже можна зробити висновки, що існує така інформація, яка потребує захисту.

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

У тому ж законі про інформацію поняття захист інформації визначається як, сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Захист – засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні, в тому числі програмні, заходи запобігання несанкціонованого доступу до апаратури, програм і даних.

Метод захисту (protection method) – система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним або апаратним способом [2].

Захист інформації ведеться з метою підтримки таких властивостей інформації як:

- цілісність – неможливість модифікації інформації неавторизованим користувачем. Цілісність інформації важливий аспект інформаційної безпеки, що забезпечує запобігання несанкціонованих змін та руйнування інформації [4].

Цілісність, це стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи; автоматичне відновлення у випадку виявлення системою потенційної помилки; автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу; [2]

- конфіденційність – інформація не може бути отримана неавторизованим користувачем. Треба захисти інформацію від несанкціонованого ознайомлення з нею.

- доступність – полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

У літературних джерелах розглядається ряд заходів для захисту інформаційної системи. Зокрема автори виділяють:

- законодавчі (закони, нормативні акти, стандарти та ін.);
- адміністративні (дії загального характеру організації, що робляться керівництвом);
- процедурні (конкретні заходи безпеки, що мають справу з людьми);
- програмно-технічні (для ідентифікації і перевірки автентичності користувачів; управління доступом; протоколювання і аудиту; криптографії; екранування та ін.).

Апаратно-програмні засоби захисту – засоби у яких програмні (мікропрограмні) та апаратні частини повністю взаємопов'язані та нероздільні.

Апаратні засоби захисту – це електронні, електромеханічні та інші пристрої, безпосередньо вбудовані у блоки автоматизованої інформаційної системи або оформлені у вигляді самостійних пристроїв які сполучаються з цими блоками. Вони призначені для внутрішнього захисту структурних елементів засобів та систем обчислюваної техніки: терміналів, процесорів, периферійного устаткування, ліній зв'язку та інше.

2.2. Інформаційна безпека комп'ютерів і комп'ютерних систем

Поняття інформаційної безпеки, залежно від його використання, розглядається у декількох ракурсах. У найзагальнішому випадку *інформаційна безпека* – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під *інформаційним середовищем* розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації.

Інформаційне середовище умовно поділяється на три основні предметні частини:

– створення і розповсюдження вихідної та похідної інформації;
– формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
– споживання інформації;

та дві забезпечувальні предметні частини:

– створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
– створення і застосування засобів і механізмів інформаційної безпеки.

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

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

В залежності від виду загроз *інформаційну безпеку* можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб; інформаційних прав і свобод людини і громадянина.

В інформаційному праві *інформаційна безпека* – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Складові інформаційної безпеки: конфіденційність, цілісність, доступність.

Конфіденційність (англ. confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

Цілісність (англ. integrity) – означає неможливість модифікації неавторизованим користувачем.

Доступність (англ. availability) – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час.

Самі механізми захисту реалізуються на трьох рівнях або шарах:

- фізичний;
- особистісний;
- організаційний.

По суті, реалізація політик і процедур безпеки покликана надавати інформацію адміністраторам, користувачам і операторам про те, як правильно використовувати готові рішення для підтримки безпеки.

2.3. Вразливість комп’ютерів і комп’ютерних систем

Під *загрозою* розуміється подія, яка потенційно може порушити одну з властивостей інформації, що захищається. Якщо джерелом загроз є діяльність людини, то говорять про порушника, якщо об'єктивні явища, то говорять про техногенні та стихійні джерела загроз.

Результатом даного етапу для виділених об'єктів повинні стати розробки окремих моделей таких видів:

– окрема модель загроз – опис загроз і схематичне представлення шляхів їх здійснення для об'єкту захисту;

– окрема модель техногенних і стихійних джерел загроз – абстрактний формалізований або неформалізований опис чинників і джерел загроз для об'єкту захисту;

– окрема модель порушника – абстрактний формалізований або неформалізований опис злочинця, здатного реалізувати загрозу (атаку) на об'єкт захисту.

Загрози для системи захисту інформації можуть класифікуватися за 9 ознаками:

1. За метою реалізації загрози:

- порушення конфіденційності інформації;
- порушення цілісності інформації (втрати від таких дій можуть бути набагато більшими, ніж при порушенні конфіденційності);
- порушення (часткове або повне) працездатності комп'ютерних систем (КС).

2. За принципом впливу на КС:

- з використанням доступу суб'єкту системи (користувача, процесу) до об'єкту (файла даних, каналу зв'язку тощо);
- з використанням прихованих каналів. Під прихованим каналом розуміється шлях передачі інформації, який дає змогу двом взаємодіючим процесам обмінюватися інформацією таким способом, що порушує системну політику безпеки.

Вплив, заснований на першому принципі, простіший, більш інформаційний, але від нього легше захиститись. Вплив на основі другого принципу відрізнається трудністю організації, меншою інформаційністю, складністю виявлення і усунення.

3. За характером впливу на КС:

- активна загроза, що веде до зміни стану системи і може здійснюватися або з використанням доступу (наприклад, до набору даних), або як з використанням доступу, так і з використанням прихованих каналів;
- пасивна загроза, що здійснюється шляхом спостереження користувачем будь-яких побічних ефектів (наприклад, від роботи програми) та їх аналіз. Прикладом пасивного впливу може бути прослуховування лінії зв'язку між двома вузлами мережі. Пасивний вплив не веде до зміни стану системи. Він завжди пов'язаний тільки з порушенням конфіденційності інформації в КС.

4. За причиною використовуваної помилки захисту. Така помилка може бути зумовлена однією з наступних причин:

- неадекватністю політики безпеки реальній КС;
- помилками адміністративного управління, під якими розуміють некоректну реалізацію або підтримку прийнятої політики безпеки КС;
- помилками в алгоритмах, у зв'язках між ними тощо, які виникають на етапі проектування програми або комплексу програм, у зв'язку з чим їх можна використовувати зовсім не так, як це описано в документації;
- помилками реалізації алгоритмів (помилками кодування), зв'язками між ними тощо, які виникають на етапі реалізації або відлагодження і які також можуть бути джерелом недокументованості.

5. За способом впливу на об'єкт атаки (при активному впливі):

- безпосередній вплив на об'єкт атаки, таким діям звичайно легко запобігти з допомогою засобів контролю доступу;
- вплив на систему дозволу (в тому числі загарбання привілеїв);
- опосередкований вплив (через інших користувачів);
- «маскарад», у цьому разі користувач присвоює собі повноваження іншого користувача, видаючи себе за нього;
- «користувач наосліп» – коли один користувач змушує іншого виконувати

необхідні дії, причому останній про них може і не підозрювати; для цього може використовуватися вірус (він виконує необхідні дії та повідомляє тому, хто його впровадив, про результат).

6. За способом впливу на КС:

- в інтерактивному режимі;
- в пакетному режимі.

7. За об'єктом атаки.

Впливам можуть піддаватися такі компоненти КС:

- КС в цілому (проникнення в систему), для цього, як правило, використовують метод «маскараду», перехоплення або підробки пароля, «злом» та доступ до КС через мережу;
- об'єкти КС – дані або програми, самі пристрої системи, канали передачі даних;
- суб'єкти КС – процеси і підпроцеси користувачів, частим випадком такого впливу є введення зловмисником вірусу в середовище другого процесу і його виконання від імені цього процесу;
- канали передачі даних – пакети даних, які передаються каналами зв'язку і власне канали, прослуховування каналу і аналіз графіка (потоку повідомлень, підміна або модифікація повідомлень у каналах зв'язку і на вузлах-ретрансляторах, зміна топології та характеристик мережі).

8. За використовуваними засобами атаки (можна використовувати або стандартне програмне забезпечення, або спеціально розроблені програми).

9. За станом об'єкта атаки. Об'єкт атаки може знаходитись в одному із трьох станів:

- збереження – вплив на об'єкт, як правило, здійснюється з використанням доступу;
- передачі – вплив передбачає або доступ до фрагментів інформації, що передається, або просто прослуховування з використанням прихованих каналів;
- обробки – об'єктом атаки є процес користувача.

Серед найпоширеніших загроз є несанкціонований доступ (НСД). Він полягає в отриманні користувачем доступу до об'єкта, який у нього немає дозволу відповідно до прийнятої організації політики безпеки.

Для того, щоб зменшити ризик від НСД, більшість систем захисту реалізує необхідні функції за допомогою відповідного набору привілеїв. Незаконне захоплення привілеїв можливе або при наявності помилок у самій системі захисту, або через халатність при управлінні системою і привілеями.

Небезпечні дії, що можуть призвести до порушення конфіденційності, цілісності та доступності певних компонентів і ресурсів КС , можна згрупувати наступним чином:

- стихійні лиха;
- зовнішні впливи (підключення до мережі, інтерактивна робота, діяння зловмисників);
- навмисні порушення;
- ненавмисні помилки (введення помилкової команди, даних, використання несправних пристроїв, носіїв, а також нехтування деякими правилами безпеки).

Види загроз, які можуть з’явитися в результаті небезпечних дій:

- розкриття (витік) інформації. Для даного виду загрози об’єктами дій є устаткування (крадіжка носіїв, підключення, несанкціоноване використання ресурсів), програми (несанкціоноване копіювання, перехоплення), дані (крадіжка, копіювання, перехоплення), персонал (передача відомостей про захист, розголошення, халатність);
- порушення цілісності інформації: устаткування (підключення, модифікація, спеціальні вкладення, зміна режимів, несанкціоноване використання ресурсів), програми (впровадження «троянських коней» та «жучків»), дані (спотворення, модифікація), персонал (вербування, підкуп персоналу, «маскарад»);
- порушення працездатності системи: устаткування (зміна режимів, виведення з ладу, руйнування), програми (спотворення, вилучення, підміна), дані (видалення, спотворення), персонал (звільнення з посади, фізичне усунення).

ТЕМА 3. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

3.1. Канали витоку інформації (атака та вторгнення в КС) та їх класифікація.
3.2. Загрози безпеці інформації в комп’ютерних системах.
3.3. Канали несанкціонованого отримання інформації в КС

3.1. Канали витоку інформації (атака та вторгнення в КС) та їх класифікація

Сучасні системи обробки таємної та конфіденційної інформації являють собою складні програмно-апаратні комплекси, що володіють специфічними каналами витоку інформації, що супроводжують штатний процес обробки інформаційних ресурсів. На рисунку 3.1 зображено класифікацію каналів витоку та перехвату інформації.

Однією із основних вимог комплексного захисту є системний підхід, тому при виявленні технічних каналів витоку інформації необхідно розглядати усю сукупність елементів захисту, включаючи основне обладнання технічних засобів обробки інформації (ТЗОІ), кінцеві пристрої, з’єднувальні лінії, розподілюючі та комутаційні пристрої, системи електропостачання, заземлення і т.п.

Поряд із основними технічними засобами, що безпосередньо залучені до обробки та передачі інформаційних ресурсів, необхідно враховувати також допоміжні технічні засоби і системи (ДТЗіС) такі, як технічні засоби відкритого телефонного, факсимільного зв’язку, системи охоронної та пожежної сигналізації, електрифікації, радіофікації, електропобутові пристрої та інші струмопровідні металоконструкції.

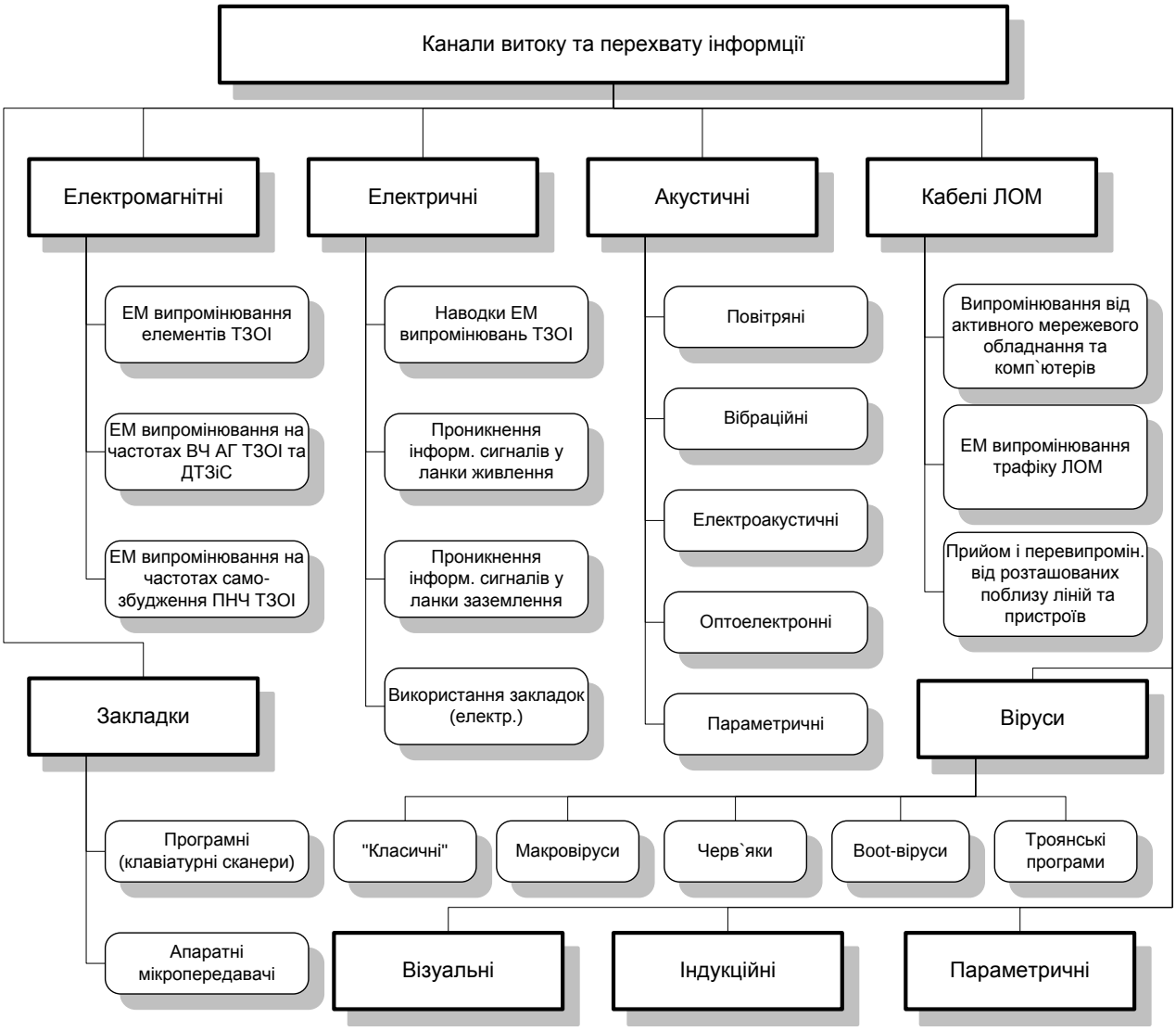

Рисунок 3.1 - Класифікація каналів витоку та перехвату інформації

Відповідно до способів перехвату інформації, від фізичної природи, а також середовища розповсюдження канали витоку та перехвату інформації можна розділити на електромагнітні, електричні, акустичні, кабелі локальних обчислювальних мереж (ЛОМ), візуальні, індукційні, параметричні, закладки та віруси (див. рисунок 3.1).

Для електромагнітних каналів характерним є побічне випромінювання таких типів:

- електромагнітне (ЕМ) випромінювання елементів ТЗОІ (носієм інформації є електричний струм, сила струму, напруга, частота або фаза якого змінюються за законом інформаційного сигналу);

- ЕМ випромінювання на частотах роботи високочастотних генераторів ТЗОІ та ДТЗіС (внаслідок зовнішніх впливів інформаційного сигналу на елементах генераторів наводяться електричні сигнали, що можуть викликати незловмисну модуляцію власних високочастотних коливань, та випромінювання

їх в оточуюче середовище);

- ЕМ випромінювання на частотах самозбудження підсилювачів низької частоти ТЗОІ (самозбудження виникає внаслідок виникнення випадкових перетворень від'ємних зворотних зв'язків в паразитні додатні, що призводить до переведення підсилювача з режиму підсилення у режим автогенерування сигналу модульованого інформаційним сигналом).

Можливими причинами виникнення електричних каналів витоку є :

- наводки ЕМ випромінювань елементів ТЗОІ (виникають при випромінюванні ТЗОІ інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ТЗОІ та побічних провідників та ліній ДТЗіС);

- проникнення інформаційних сигналів в мережі електропостачання (можуть виникати при наявності магнітного зв'язку між вихідним трансформатором підсилювача та трансформатором електропостачання, а також за рахунок нерівномірного навантаження на випростувальний пристрій, що приводить до зміни споживаного струму за законом зміни інформаційного сигналу);

- проникнення інформаційних сигналів в ланки заземлення (можуть виникати при наявності гальванічного зв'язку із заземленням різноманітних провідників, що виходять за межі зони контролю, в тому числі нульового проводу мережі електропостачання, екранів, металевих труб систем опалення та водопостачання, металевої арматури і т.п.);

- перехват інформації з використанням закладних пристроїв (являють собою міні передавачі, що встановлюються в ТЗОІ, випромінювання яких модулюються інформаційним сигналом і приймаються за межами зони контролю).

Середовищем акустичних каналів витоку та перехвату інформації можуть бути повітря, конструкції будівель, труби водопостачання та опалення, а також інші тверді тіла. Серед акустичних каналів виділяють:

- повітряні (носієм інформації є повітря і для їх перехвату використовують мініатюрні високочутливі та вузько напрямлені мікрофони, що з'єднанні з диктофонами чи спеціальними міні-передавачами);

- вібраційні (носієм інформації є вібруючі конструкції будівель в межах зони контролю, а для перехоплення інформації використовують контактні, електронні та радіостетоскопи);

- електроакустичні (утворюються за рахунок перетворення акустичних сигналів в електричні, наприклад в телефонних апаратах з електромеханічними дзвінками);

- оптоелектронні (утворюються при опроміненні лазерним променем вібруючих в акустичному полі тонких відбиваючих поверхонь, наприклад віконне скло, дзеркала, картини і т.п.);

- параметричні (утворюються в результаті дії акустичного поля на елементи високочастотних генераторів та зміні взаємно розміщення елементів схем, провідників, дроселів і т.п., що призводить до зміни параметрів сигналу).

Слід зауважити, що акустичні канали можуть бути джерелом витоку не

лише мовної інформації, але й інформації з механічних замків, ключів, інформації з принтера чи клавіатури комп'ютера тощо.

Кабелі ЛОМ виділені в окрему групу, оскільки сучасні системи обробки інформації побудовані на базі локальних комп'ютерних мереж і, як правило, таке кабельне господарство являє собою розвинуту мережу провідників різного типу. Кабельна система не містить в собі активних чи нелінійних елементів, тому сама по собі вона не може бути джерелом «побічних» випромінювань, проте кабельна система пов'язує між собою всі елементи комп'ютерної мережі. По ній передаються мережеві дані, але також вона є і приймачем усіх паразитних наведень і середовищем для переносу побічних ЕМ випромінювань. Розрізняють такі причини виникнення каналів витоку та перехоплення інформації:

- випромінювання від активного мережевого обладнання та комп'ютерів (внаслідок неоднорідності кабельної системи та заземлення інформація від клавіатури чи монітора може випромінюватися мережевою системою);
- ЕМ випромінювання трафіку ЛОМ (існує множина атак спрямованих на аналіз трафіку ЛОМ для визначення критичних ділянок навантаження системи, тому така інформація є важливою для зловмисника);
- прийом і перевипромінювання від розташованих поблизу ліній та пристроїв (кабельна система може розглядатися як антена для перевипромінювання інших пристроїв, наприклад телефонних чи факсимільних апаратів, модемів та ін.).

Візуальні канали витоку інформації широко використовувалися в епоху до-комп'ютерного захисту інформації та продовжують застосовуватися і тепер. Для цього використовують спеціальні технічні засоби оптичного, теплового та іншого випромінювання. Для документування результатів спостереження проводять фотографування чи зйомку об'єктів. Для дистанційного збору інформації використовують відео-закладки.

Індукційний канал перехоплення інформації не потребує контактного підключення до каналів зв'язку, тому він найчастіше використовується для маскування самого процесу зйому інформації. Сучасні індукційні здавачі можуть знімати інформацію з кабелів, захищених не лише ізоляцією, але також і подвійною стальною стрічкою з стальним дротом, що щільно обвивають кабель.

Параметричний канал витоку інформації формується шляхом високочастотного опромінення елементів ТЗОІ, при взаємодії магнітного поля котрого із елементами ТЗОІ виникає перевипромінення електромагнітного поля, промодулюваного інформаційним сигналом.

Закладка - це спеціальний засіб, призначений для збору та подальшої ретрансляції конфіденційної чи таємної інформації. В сучасних комп'ютерних засобах можуть використовуватися як програмні, так і апаратні закладки (наприклад, програмні клавіатурні шпигуни, апаратні мікро радіопередавачі та ін.). Зрозуміло, що складність виявлення таких закладних засобів безпосередньо впливає на захищеність комп'ютерних інформаційних ресурсів, що знаходяться в системі.

На рисунку 3.2 зображено узагальнену класифікацію атак спеціального виду на криптопристрої.

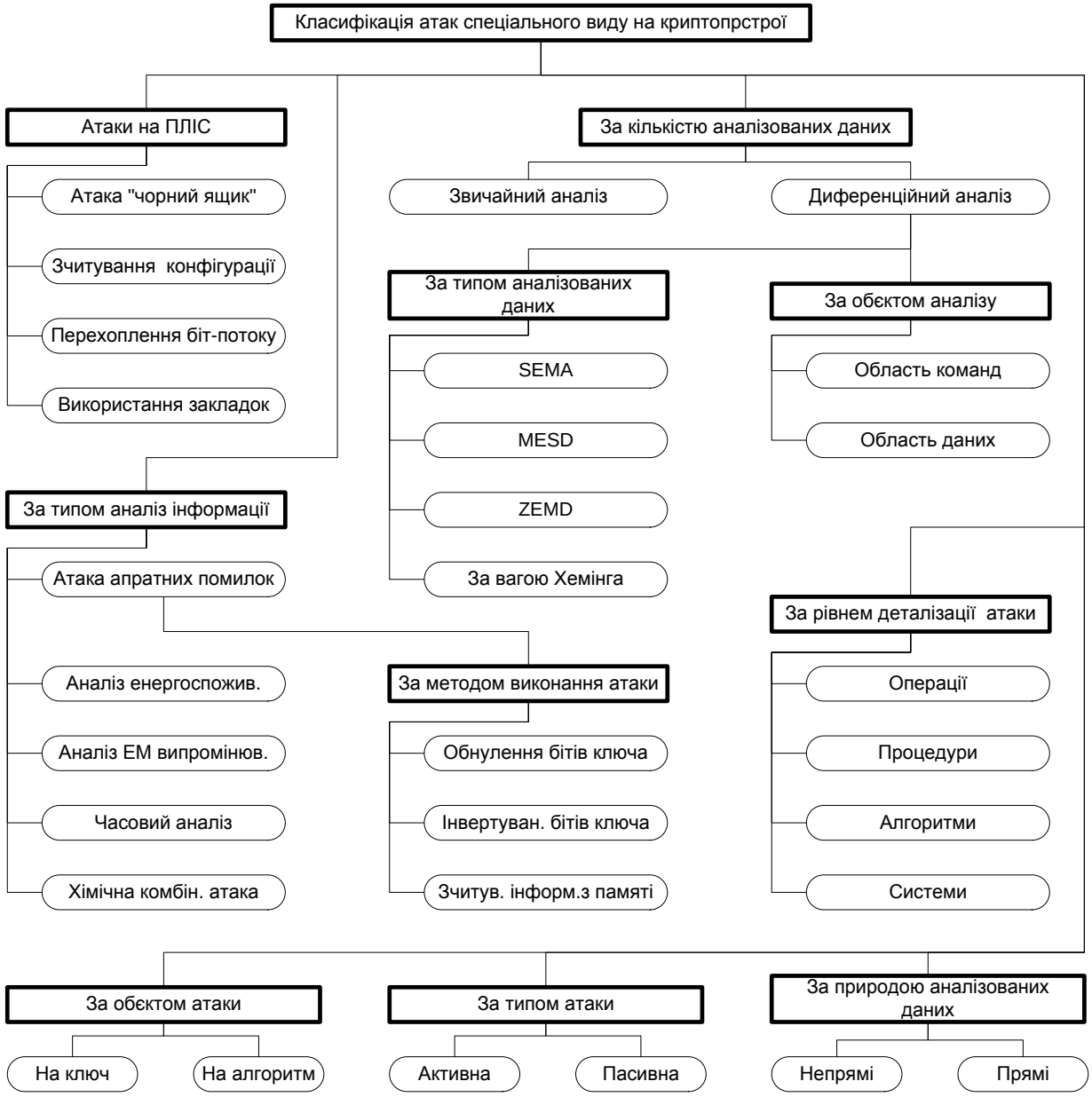

Рисунок 3.2 - Узагальнена класифікація атак спеціального виду на криптопристрої

У якості ключових ознак наведено такі:

- за типом аналізованої інформації – дана ознака є найпопулярнішою і широко використовується для визначення який саме тип інформації з побічних каналів витоку лежить в основі криптоаналізу. Розрізняють такі види: атака апаратних помилок, аналіз енергоспоживання, аналіз електромагнітного випромінювання, часовий аналіз, хімічна комбінаторна атака;

- за методом виконання атаки – у свою чергу атака апаратних помилок в залежності від методики проведення спеціальних впливів на апаратуру може містити відмінні ключові операції самого криптоаналізу, тому розрізняють такі види: обнулення бітів ключа, інвертування бітів ключа, зчитування інформації з пам’яті;

- за кількістю аналізованих даних розрізняють звичайний та диференційний

аналіз. Для звичайного аналізу достатньо лише одного (або кількох) сигналу, а диференційний аналіз використовують, щоб за допомогою статистичних методів усереднити та усунути випадкові та зумисні завади та виділити корисний сигнал з каналів витоку;

- за типом аналізованих даних диференційний аналіз ділиться на такі: за вагою Хемінга, SEMD – Simple Exponent Multiply Data (одна експонента, багато даних), MESD – Multiply Exponent Simple Data (багато експонент, одне дане), ZEMD – Zero Exponent Multiply Data (жодної експоненти, багато даних);

- за об'єктом аналізу розрізняють атаки на область команд та на область даних. Атаки на область команд мають за мету змінити порядок виконання операцій алгоритму;

- за рівнем деталізації атаки охоплюють усю ієрархію сучасних систем захисту інформації на рівні операцій, процедур, алгоритмів та цілої системи захисту;

- за об'єктом атаки поділяють на атаки на ключ та на алгоритм. У деяких випадках зловмиснику корисно атакувати не ключ, а сам алгоритм, наприклад, зменшити до мінімуму (однієї) кількість ітерацій і застосувати алгоритми квазі-повного перебору;

- за типом атаки бувають пасивні, коли зловмисник лише накопичує та аналізує дані, отримані по каналах витоку (наприклад, при часовому аналізі), та активні, у випадку коли зловмисник спеціальним чином діє на криптографічний пристрій, щоб спричинити появу каналів витоку, які за нормальних умов експлуатації не проявляються (наприклад, атака апаратних помилок);

- за природою аналізованих даних розрізняють прямі, у випадку коли отримані сигнали безпосередньо стосуються аналізованих криптографічних операцій (наприклад, при аналізі енергоспоживання), а також коли використовуються непрямі, модульовані, відбиті сигнали (наприклад, при аналізі електромагнітного випромінювання) .

3.2. Загрози безпеці інформації в комп'ютерних системах

Загрози циркулюючої в КС інформації, як правило, залежать від структури та конфігурації КС, технології обробки інформації в ній, стану навколишнього фізичного середовища, дій персоналу і структури самої інформації.

З множини способів класифікації загроз інформації найбільш узагальненою (базовою) є їх класифікація за наслідками можливого впливу на інформацію:

- загрози порушення конфіденційності;
- загрози порушення цілісності;
- загрози порушення доступності.

Загрози конфіденційності направлені на розголошування конфіденційної або секретної інформації. У разі реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу.

Загроза порушення конфіденційності має місце кожного разу, коли можливий несанкціонований доступ до певної закритої інформації, що

зберігається в комп'ютерній системі або передається від однієї системи до іншої.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання.

Загрози цілісності інформації направлені на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена умисно, а також у результаті об'єктивних дій з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації, комп'ютерних мереж і систем телекомунікацій. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція певної бази даних).

Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (знищення).

Загрози доступності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні умисні дії або знижують працездатність КС, або блокують доступ до деяких її ресурсів.

Наприклад, якщо один користувач системи запитує доступ до певної служби, а інший чинить дії, які призводять до блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсів може бути постійним або тимчасовим.

Крім того, серед основних загроз інформації можуть бути наступні:

- розкрадання, перехоплення (копіювання інформації);
- знищення інформації;
- модифікація (перекручування) інформації;
- порушення доступності (блокування) інформації;
- заперечення дійсності інформації (фальсифікація);
- нав'язування помилкової інформації.

Інформація зберігає доступність, якщо зберігається можливість її отримання або модифікації тільки відповідно до встановлених правил упродовж певного часу.

Отже, загрози, реалізація яких призводить до втрати інформацією вказаних вище властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації.

3.3. Канали несанкціонованого отримання інформації в КС

Канали несанкціонного отримання доступу до інформації це такі дестабілізуючі чинники, наслідком проявлення яких може бути отримання (або небезпека отримання) інформації, яка захищається, особами або процесами, що не мають на це законних прав (повноважень).

Основними типами каналів несанкціонного доступу до інформації є:

1. Канали, що відносяться безпосередньо до опрацювання інформації і без доступу зловмисника до елементів та вузлів комп’ютерної техніки:

- викрадення носіїв інформації, прослуховування розмов осіб, які мають відношення до КС (чи ІС);
- провокація на розмови осіб причетних до КС (чи ІС);
- використання зловмисником візуальних засобів;
- використання зловмисником оптичних засобів;
- використання зловмисником акустичних засобів.

2. Канали, які виявляються в процесі опрацювання інформації без доступу зловмисника до елементів КС:
- електромагнітні випромінювання пристроїв відображення інформації, процесорів, зовнішніх запам'ятовуючих пристроїв, апаратури зв'язку, ліній зв'язку, допоміжної апаратури;
- паразитні наведення в системах телефонного та диспетчерського зв'язку, в мережах живлення (50 Гц), в шинах заземлення;
- підключення генераторів завад, апаратури реєстрації;
- огляд відходів виробництва, що потрапляють за межі контрольованої зони.

3. Канали, які виявляються і не відносяться до опрацювання інформації з доступом зловмисника до елементів КС, але без зміни останніх:
- копіювання бланків з вихідними даними, магнітних носіїв, з пристроїв відображення, вихідних документів та ін.;
- викрадення виробничих відходів.

4. Канали, які виявляються в процесі опрацювання інформації з доступом зловмисника до елементів КС, але без зміни останніх:
- запам'ятовування інформації із бланків з вихідними даними, з пристроїв наочного відображення, інформації на вихідних документах, службових даних;
- копіювання інформації в процесі опрацювання;
- копіювання дублікатів масивів і вихідних документів;
- копіювання роздруку масивів;
- використання програмних пасток;
- ‘
- використання недоліків систем програмування;
- використання недоліків операційних систем.

5. Канали, що мають пряме відношення до опрацювання інформації з доступом зловмисника до елементів комп'ютерної техніки із зміною останніх:
- підміна носіїв інформації, первинних документів, апаратури;
- підміна елементів (фрагментів) програм, елементів баз даних.

6. Канали, які виявляються в процесі опрацювання інформації з доступом зловмисника до об'єктів комп'ютерної техніки із зміною її елементів:
- незаконне підключення до апаратури, ліній зв'язку;
- зняття інформації з процесорів, апаратури зв'язку, ліній зв'язку, зовнішніх запам'ятовуючих пристроїв, допоміжної апаратури.

ТЕМА 4. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Завдання захисту інформації.
4.2. Проблеми захисту інформації в комп'ютерних системах.
4.3. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності.
4.4. Поняття і класифікація комп'ютерних вірусів.

4.1.Завдання захисту інформації

Широке застосування комп'ютерних технологій в ком'ютерних системах та мережах, автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаною з носієм, може легко і швидко копіюватись та передаватись через канали зв'язку. Відома дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх, так і з боку внутрішніх порушників режиму таємності.

Безпека інформації в інформаційній системі чи телекомунікаційній мережі забезпечується здатністю цієї системи зберігати таємність інформації при її введенні, виведенні, передаванні, обробці та зберіганні, а також протистояти її руйнуванню, крадіжкам чи спотворенню. Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехвату, спотворення чи введення помилкової інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні посідають центральне місце в системі забезпечення безпеки інформації в інформаційних системах та телекомунікаційних мережах.

Завданням забезпечення безпеки (захисту) інформації є:

- захист інформації в каналах зв'язку та базах даних криптографічними методами;
- підтвердження справжності об'єктів даних та користувачів (аутентифікація сторін, що встановлюють зв'язок);
- виявлення порушень цілісності об'єктів даних;
- забезпечення захисту технічних засобів та приміщень, в яких ведеться обробка конфіденційної інформації, від витоку через побічні канали і від можливо вбудованих в них електронних пристроїв знімання інформації;
- забезпечення захисту програмних продуктів та засобів обчислювальної техніки від внесення в них програмних вірусів та закладок;
- захист від несанкціонованих дій через канал зв'язку від осіб, що не допущені до засобів шифрування, але що переслідують цілі компрометації таємної інформації і дезорганізації роботи абонентських пунктів;
- організаційно-технічні заходи, спрямовані на забезпечення збереження інформації з обмеженим доступом;

- виконання вимог з кібербезпеки в інформаційних мережах.

4.2. Проблеми захисту інформації в комп’ютерних системах

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми - комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби. Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є наступні:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників КС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

У сфері захисту інформації та комп’ютерної безпеки в цілому найбільш актуальними є три групи проблем:

- порушення грифу обмеження доступу;
- порушення цілісності інформації;
- порушення дієздатності інформаційно-обчислювальних систем.

Захист інформації перетворюється у найважливішу проблему державної безпеки, коли мова йде про державну, дипломатичну, військову, промислову, медичну, фінансову та іншу таємну інформацію. Величезні масиви такої інформації зберігаються в електронних архівах, оброблюються в інформаційних системах та передаються через телекомунікаційні мережі. Основні властивості цієї інформації – конфіденційність та цілісність, повинні підтримуватись законодавчо, юридично, а також організаційними, технічними та програмними методами.

Згідно із Законом України «Про захист інформації в автоматизованих системах» *захист інформації* - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. У літературі вживаються також

споріднені терміни «безпека інформації» та «безпека інформаційних технологій».

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно- технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту.

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними причинами порушення безпеки інформації можна назвати такі:

- несанкціонований доступ - доступ до інформації, що здійснюється з порушенням установлених в КС правил розмежування доступу;
- витік інформації - результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації - дія, внаслідок якої інформація в КС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації - навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в КС;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи КС - дії або обставини, які призводять до спотворення процесу обробки інформації. Причини настання зазначених випадків такі:
- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
- некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1С, спричинення витоку інформації);
- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією). Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту. Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви:

- сторонні, які не знають фірму;
- сторонні, які знають фірму, та колишні співробітники;
- співробітники-непрограмісти;
- співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на сайтах Інтернет та ін.

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: *«хакери», «кракери», «пірати», «шкідники».*

Хакери (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи.

У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів КС тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів — кракерів (або «крекерів»), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

Найбільш криміногенною групою є *пірати* — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку. В усіх випадках мотивація – матеріальні інтереси. За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів.

Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль. Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш

тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про експериментаторів («піонерів»). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні. Отже, одними з основних причин порушення безпеки інформації є незапитаність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.

4.3. Види комп’ютерних злочинів. Причини поширення комп’ютерної злочинності

Проблема комп’ютерної злочинності та розробка механізмів протидії привернула до себе увагу провідних криміналістів ще з часів широкого впровадження комп’ютерної техніки. Статистка таких злочинів велася з 1958 р. Тоді їх розуміли як випадки псування і розкрадання комп’ютерного устакування; крадіжку інформації; несанкціоноване використання комп’ютерів; шахрайство або крадіжку, вчинене за допомогою комп’ютерів. У 1996 р. комп’ютер уперше був використаний як інструмент для пограбування банку (Мінесота). Нині високотехнологічна злочинність набуває високих темпів. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України). Найбільш поширеними видами комп'ютерних злочинів є:

1. Несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання. Розрізнити ці дві категорії дуже важко. Найчастіше присвоєння комп’ютерної інформації та програмного забезпечення відбувається копіюванням, що зменшує ймовірність виявлення факту крадіжки. Можливими шляхи здійснення злочину є:

- використання чужого імені або пароля («маскарад»). Одержати коди та паролі законних користувачів можна придбанням (звичайно з підкупом персоналу) списку користувачів з необхідними відомостями, знаходженням

подібного документа в організаціях, де контроль за їх збереженням недостатній;

- підслуховуванням через телефонні лінії. Відомі випадки, коли секретна інформація, і не тільки приватного характеру, відпливала через дітей;

- незаконне використання привілейованого доступу;

- «зламування» системи;

- знаходження слабких місць у захисті системи чи недоробок у програмному забезпеченні;

- використання збоїв системи;

- крадіжка носіїв інформації; - читання інформації з екрана монітора;

- збирання «сміття»;

- встановлення апаратури підслуховування та запису, підімкненої до каналів передавання даних;

- віддалене підімкнення;

- модифікація програмного забезпечення

2. Підробка комп'ютерної інформації. Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник КС. В останньому випадку може підроблятись вихідна інформація з метою імітування роботоздатності КС і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.

3. Введення у програмне забезпечення «логічних бомб» - невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьо вує в певний момент часу. Ще одним способом модифікації програмного забезпечення є таємне введення у програму (чужу або свою) *«троянського коня»* — команд, які дають можливість зі збереженням працездатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянській кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянській кінь», а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, а й в інших файлах, наприклад в електронних листах.

4. Розробка і поширення комп'ютерних вірусів. Напевне, сьогодні не має жодного користувача КС, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будь- якому разі це означає порушення цілісності КС. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.

5.Злочинна недбалість у розробці, виготовленні та експлуатації комп'ютерної техніки та програмного забезпечення. Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим

видом техніки, транспорту і т. Його особливістю є те, що безпомилкових програм не буває в принципі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців, та про винність розробників свідчать:

- наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призводить до збою (аварії);

- можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії). Окремим випадком недбалості програмістів є створення і залишення без контролю *«люків»* («чорних ходів») — прихованих, не задокументованих точок входу у програмний модуль, які часто використовуються для відлагодження програми та її підтримання у процесі використання. Однак «люк» може бути використаний і для зламування системи сторонньою особою, і для таємного доступу до програми самим розробником. Для виявлення «люків» слід проводити ретельний аналіз початкових текстів програм. До тяжких непередбачуваних наслідків можуть призвести й дії користувачів.

6. Комп'ютерні злочини в мережі Інтернет. Ввідокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це промисловий шпіонаж, саботаж, поширення дитячої порнографії і т. ін. Понад третина користувачів Мережі страждає від шахрайств.

Одним із ключових аспектів багатьох «схем» подібного роду є доступ до персональних даних користувача. Заповнивши анкету, людина стає потенційним об'єктом шахрайства в майбутньому, а найбільш довірливі, зокрема ті, хто надає інформацію про свою кредитну картку, страждають відразу. Відомо, що більшість шахрайств пов'язана з використанням пластикових кредитних карток і здійснюється на сайтах, що спеціалізуються на купівлі-продажу товарів. По-друге, стає все більше злочинів, пов'язаних із самим існуванням Інтернет.

Фактично єдиний спосіб створити систему, абсолютно стійку до зовнішніх впливів, - припинити будь-які її зв'язки із зовнішнім світом. А мінімальним із погляду заходом є заборона доступу до Інтернет не для службових цілей.

Злочини, що вчиняються організованими злочинними угрупуваннями з використанням ІТ:

1) злочини насильницького характеру та інші злочини, які є потенційно небезпечними;

2) злочини ненасильницького характеру (як правило, економічного).

Злочини І категорії: *Кібертероризм* – тероризм спланований, вчинений чи скоординований в кіберпросторі, тобто в терористичних акціях використовуються новітні досягнення науки і техніки в галузі ІТ.

Злочини ІІ категорії:

- «відмивання» грошей;
- крадіжка грошей з банківських рахунків;
- шахрайські операції з пластиковими платіжними картками;
- розповсюдження інформації про наркотики через Інтернет.

4.4. Поняття і класифікація комп’ютерних вірусів

Вважають, що перші прототипи «електронних інфекцій» з'явились наприкінці 1960-х - на початку 1970-х років у вигляді програм-«кроликів», які швидко розмножувались і займали системні ресурси, знижуючи таким чином, продуктивність комп'ютерів.

Термін «комп'ютерний вірус» уперше вжив американський студент Фред Коен у 1984 році. Він поділив віруси на дві великі групи. До першої він відніс ті, які написані для певних наукових досліджень у галузі інформатики, а до другої — «дикі» віруси, розроблені з метою заподіяння шкоди користувачам. Сьогодні написання вірусів набуває ознак промислового виробництва, їх кількість вимірюється десятками тисяч, і розуміння цієї загрози має стати необхідною вимогою для кожного користувача. Комп'ютерний вірус — спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області і т. ін. (заражати їх), та виконувати різноманітні небажані дії. Небезпечність вірусу зростає через наявність у нього латентного періоду, коли він не виявляє себе. Для маскування вірус може використовуватися разом з «логічною» або «часовою бомбою».

Кілька ознак зараження КС вірусами:

- припинення роботи або неправильна робота програм, які раніше функціонували успішно;
- неможливість завантаження операційної системи;
- зменшення вільного обсягу пам'яті;
- уповільнення роботи комп'ютера;
- затримки під час виконання програм, збої в роботі комп’ютера;
- раптове збільшення кількості файлів на диску;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- незрозумілі зміни у файлах;
- зміни дати і часу модифікації файлів без очевидних причин;
- незрозумілі зміни розмірів файлів;
- видача непередбачених звукових сигналів;
- виведення на екран непередбачених повідомлень або зображень.

Віруси можна класифікувати за різними ознаками. За середовищем існування розрізняють файлові, завантажувальні, комбіновані (файлово-завантажувальні), пакетні та мережні віруси.

Файлові віруси звичайно заражають файли з розширеннями .com та .exe. Однак, деякі їх різновиди можуть інфікувати файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), при цьому вони, як правило, втрачають здатність до розмноження. У свою чергу, за способом зараження середовища існування файлові віруси поділяють на резидентні та нерезидентні. Останні починають діяти тільки під час запуску зараженого файла на виконання і залишаються активними обмежений час. Резидентні віруси інсталюють свою копію в оперативній пам'яті, перехоплюють звертання опе- раційної системи до різних об'єктів і заражають їх. Деякі віруси здатні перехоплювати досить багато різних функцій переривань, У результаті чого файли можуть заражатись у процесі перейменування, копіювання,

знищення, змінювання атрибутів, перегляду каталогів, виконання, відкривання та здійснення інших операцій. Резидентні віруси зберігають активність весь час до вимикання комп' ютера.

Порівняно новою групою можна назвати макровіруси, які використовують можливості макромів, вбудованих у текстові редактори, електронні таблиці і т. ін. Нині поширені макровіруси у Microsoft Word і Excel. Вони перехоплюють деякі файлові функції в разі відкриття чи закриття зараженого документа і згодом інфікують решту файлів, до яких звертається програма. У певному сенсі такі віруси можна назвати резидентними, оскільки вони активні тільки у своєму середовищі - відповідному додатку.

Завантажувальні віруси відрізняються від файлових резидентних вірусів тим, що вони переносяться із системи в систему через завантажувальні сектори. Комп'ютер заражається таким вірусом після спроби завантаження системи з інфікованого диска, а дискета - при читанні її «змісту».

Комбіновані віруси можуть поширюватись як через завантажувальні сектори, так і через файли.

Пакетні віруси - це порівняно прості і старі віруси, написані мовою управління завданнями операційної системи.

Мережні віруси («черв'яки») розмножуються по комп'ютерній мережі, зменшуючи тим самим її пропускну здатність, уповільнюючи роботу серверів і т. ін. Вони посідають перше місце за швидкістю поширення. Найбільш відомим є так званий «*черв'як Морріса*». Останні моделі «черв'яків» упроваджуються у різні архіви (arj, zip та ін.) і зменшують вільний простір на диску. За ступенем дистуктивності віруси можна поділити на такі групи:

- порівняно безпечні, нешкідливі - їх вплив обмежується зменшенням вільної пам'яті і графічними або звуковими ефектами. Варто зазначити, що зменшення пам'яті в деяких випадках може призвести до збою системи, а ефекти - відволікти користувача, у результаті чого він припуститься помилки;
- небезпечні - віруси, які можуть призводити до збійних ситуацій;
- дуже небезпечні - дії вірусів можуть призвести до втрати програм, знищення даних, стирання інформації в системних областях тощо. За особливостями алгоритму віруси важко класифікувати через їх різноманітність. Можна виокремити найпростіші, «вульгарні» віруси, написані єдиним блоком, який можна розпізнати в тексті програми-носія, та віруси «роздроблені» — поділені на частини, що нібито не мають між собою зв'язку, але містять інструкції комп'ютерові, як їх зібрати в єдине ціле і розмножити вірус.

З погляду прийомів маскування розрізняють *віруси-невидимки* (стелс-віруси, stealth) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за роботу з файлами, і коригують результати звернень. Механізм «невидимості» в кожному з цих вірусів реалізується по-своєму, однак можна виокремити кілька загальних принципів:

- для приховування збільшення довжини заражених файлів вірус передає програмі перегляду каталогів зменшене значення їхньої довжини;
- для того щоб користувач не виявив код вірусу під час перегляду файла, вірус виліковує його в момент відкриття і заново заражає у процесі закриття;

- для того щоб замаскувати свою присутність у пам'яті комп'ютера, вірус стежить за діями резидентних моніторів пам'яті, у разі спроби перегляду коду вірусу система зависає.

Поліморфними називають віруси, які застосовують різноманітні способи шифрування власного тіла. У разі зараження чергового файла алгоритм шифрування змінюється випадковим чином. При цьому дуже важко виділити сигнатуру - характерну послідовність байтів у коді вірусу.

ТЕМА 5. ОСНОВНІ ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

5.1. Стратегія та архітектура захисту інформації.
5.2. Політика безпеки інформації.
5.3. Види забезпечення безпеки інформації.

5.1. Стратегія та архітектура захисту інформації

Концепція захисту інформації

Вразливість інформації в КІС обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленністю, довгостроковим збереженням великого об’єму інформації на магнітнита оптичних носіях, одночасним доступом ресурсів багатьох користувачів. В даних умовах необхідність вживання заходів захисту не викликає сумнівів. Однак існують певні труднощі:

- немає єдиної теорії захисту систем;
- розробники засобів захисту, в основному, пропонують окремі методології для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;
- для забезпечення надійного захисту необхідно вирішувати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

Для подолання перерахованих труднощів,необхідна координація дій всіх учасників інформаційного процесу як на окремому підприємстві, так і на державному рівні.

Концепція захисту інформації - офіційно прийнята система поглядів на на проблему інформаційної безпеки і шляхи її вирішення з урахуванням розробки сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів для її реалізації.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації і далі – політика безпеки інформації (рисунок 5.1).

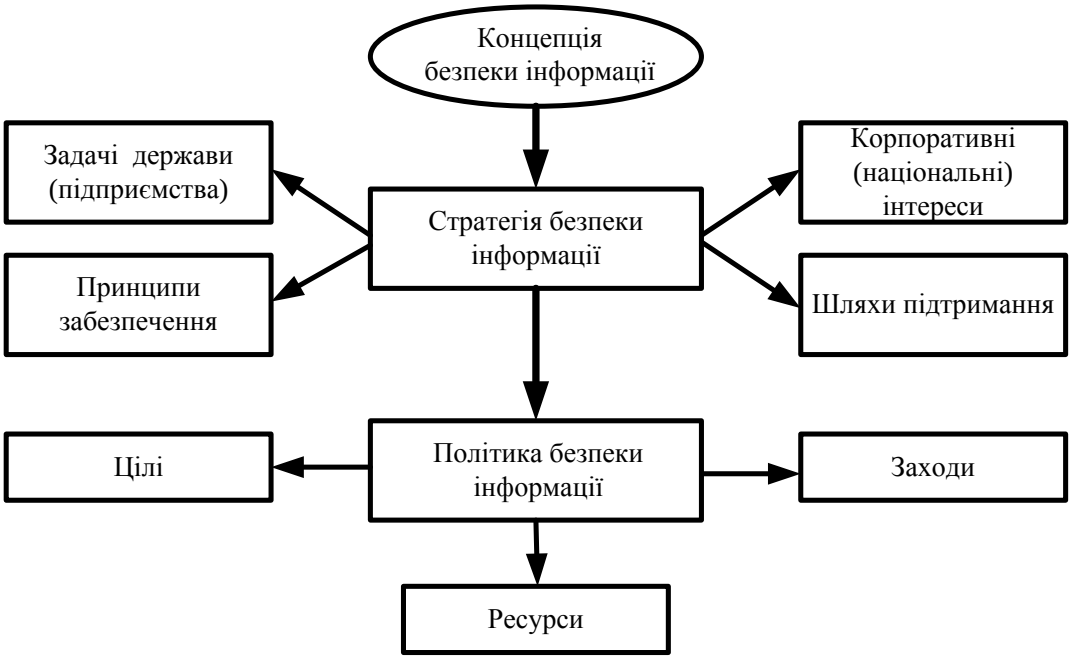

Рисунок 5.1 – Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендується проводити в три етапи, як показано на рисунку 5.2.

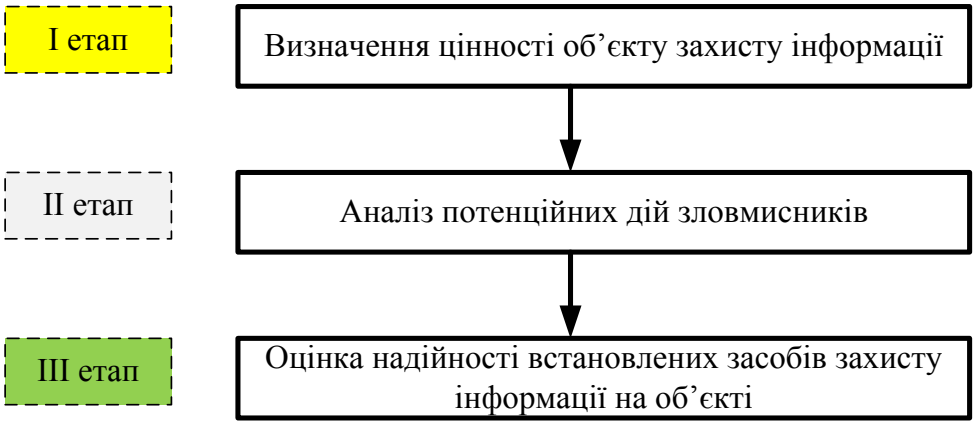

Рисунок 5.2 – Етапи розробки концепції захисту інформації

На першому етапі чітко визначається цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На даному етапі доцільно диференціювати, за значимістю, окремі об’єкти, які підлягають захисту.

Другий атап. Проведення скурпульозного аналізу злочинних дій, які потенційно можуть бути здійснені стосовно об’єкту, котрий слід захистити. Важливо визначити ступінь реальної небезпеки найбільш поширених злочинів (економічне шпигунство, саботаж, крадіжки зі взломом і тп.) та проаналізувати найбільш ймовірні дії зловмисників стосовно об’єктів, які потребують захисту.

Головною метою третього етапу є аналіз обставин, в тому числі місцевих специфічних умов, виробничих процесів, уже всановлених технічних засобів захисту.

Концепція захисту повинна містити перелік організаційних, технічних та інших заходів, які забезпечують максимальну безпеку при заданому залишковому ризику при мінімальних затратах на їх реалізацію.

Політика захисту – це загальний документ, в якому перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Політика захисту повинна обов'язково включати:

- контроль доступу (зоборона на доступ користувача до матеріалів, якими йому не дозволено користуватися);
- ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);
- ведення обліку (запис усіх дій користувача в мережі);
- контрольний журнал (журнал дозволяє визначити час і місце порушення умов захисту);
- надійність (запобігання монополізації ресурсів системи одним користувачем).

5.2. Політика безпеки інформації

При розробці політики безпеки інформації, на початковому етапі визначають об'єкти, які неохідно захистити та їх функції. При цьому, розробка політики безпеки інформації повинна проводитися з урахуванням задач, рішення яких забезпечить реальний захист даного об'єкту (рисунок 5.3).

Інформаційну систему можна вважати захищеною, якщо всі операції виконуються у відповідності з чітко визначеними правилами, як показано на рисунку 5.4, що забезпечують безпосередній захист об'єктів, ресурсів і операцій. Основу для формування вимог до захисту складає перелік загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і заходи захисту.

Отже, захист інформації в КС чи мережі ефективніший в тому випадку, коли проектування і реалізація системи захисту відбувається в три етипи:

- аналіз ризику;
- реалізація політики безпеки;
- підтримка політики безпеки.

На першому етапі аналізуються вразливі елементи КС (КМ), визначаються і оцінюються загрози та підбираються оптимальні засоби захисту. Аналіз ризику закінчується прийняттям політики безпеки.

Політикою безпеки називається комплекс взаємозалежних засобів, спрямованих на забезпечення високого рівня безпеки.

Вразливість означає невиконання хоча б однієї з цих властивостей. Для комп'ютерних мереж (систем) можна виділити наступні *ймовірні загрози* , які необхідно враховувати при визначенні політики безпеки:

Рисунок 5.3 – Комплекс задач при розробці політики безпеки

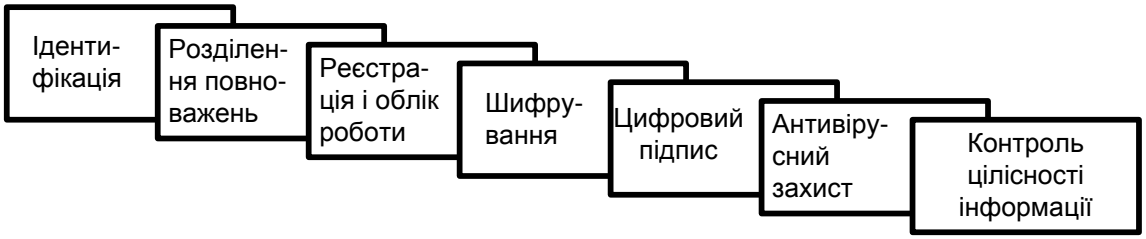

Рисунок 5.4 – Основні правила забезпечення політики безпеки інформації

- несанкціонований доступ сторонніх осіб, які не належать до числа

штатних працівників, і ознайомлення їх з конфіденційною інформацією;

- ознайомлення свого персоналу з інформацією, до якої він не повинен мати доступу;
- несанкціоноване копіювання програм і даних;
- перехоплення і ознайомлення з конфіденційною інформацією, переданою по каналах зв'язку;
- крадіжка носіїв, яка містять конфіденційну інформацію;
- крадіжка роздрукованих документів;
- випадкове або навмисне знищення інформації;
- несанкціонована модифікація документіві баз даних;
- фальсифікація повідомлень, переданих по каналах зв'язку;
- помилки в роботі обслуговуючого персоналу;
- руйнування файлової структури через некоректну роботу програм або апаратних засобів;
- руйнування програм вірусними впливами;
- руйнування архівної інформації, яка зберігається на носіях;
- крадіжка устаткування;
- помилки в програмному забезпеченні;
- відключення електроживлення;
- збої устаткування тощо.

Другий етап – реалізація політики безпеки - починається з проведення розрахунку фінансових витрат і вибору відповідних засобів для виконання цих задач. При цьому, необхідно врахувати такі фактори як: безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість отримання повної інформації про механізми захисту і надані гарантії. Крім того, варто враховувати *принципи, в яких відображені основні положення по безпеці інформації:*

- економічна ефективність (вартість засобів захисту повинна бути меншою, ніж розміри можливого збитку);
- простота (захист буде тим ефективнішим, чим легше користувачеві з ним працювати;
- відключення захисту;
- відкритість проектування і функціонування механізмів захисту (фахівці, які мають відношення до системи захисту, повинні цілком уявляти собі принципи її функціонування та, у випадку виникнення не штатних ситуацій, адекватно на них реагувати);
- незалежність системи захисту від суб'єктів захисту (особи, які займалися розробкою системи захисту, не повинні бути в числі тих, кого ця система буду контролювати);
- звітність і підконтрольність (система захисту повинна надавати досить доказів, які показують коректність її роботи);
- відповідальність (особиста відповідальність осіб, які займаються забезпеченням безпеки);
- ізоляція і поділ (об'єкти захисту доцільно розділяти на групи таким чином, щоб порушення захисту в одній з груп не впливало на безпеку інших груп)

та ін.

Підтримка політики безпеки – третій, найбільш важливий, етап. Заходи, проведені на даному етапі, вимагають постійного спостереження за вторгненнями у мережу зловмисників, виявлення слабких місць у системі захисту об’єкту інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку політики безпеки КМ чи інформаційної системи лежить на системному адміністраторі, який повинен оперативно реагувати на всі випадки злому, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту.

5.3. Види забезпечення безпеки інформації

Всі заходи протидії комп’ютерним злочинам, що безпосередньо забезпечують безпеку інформації можна поділити на:

- правові;
- організаційно-адміністративні;
- інженерно-технічні.

До правових заходів (рисунок 5.5) слід віднести розробку норм, які встановлюють відповідальність за комп’ютерні злочини, захист авторських прав

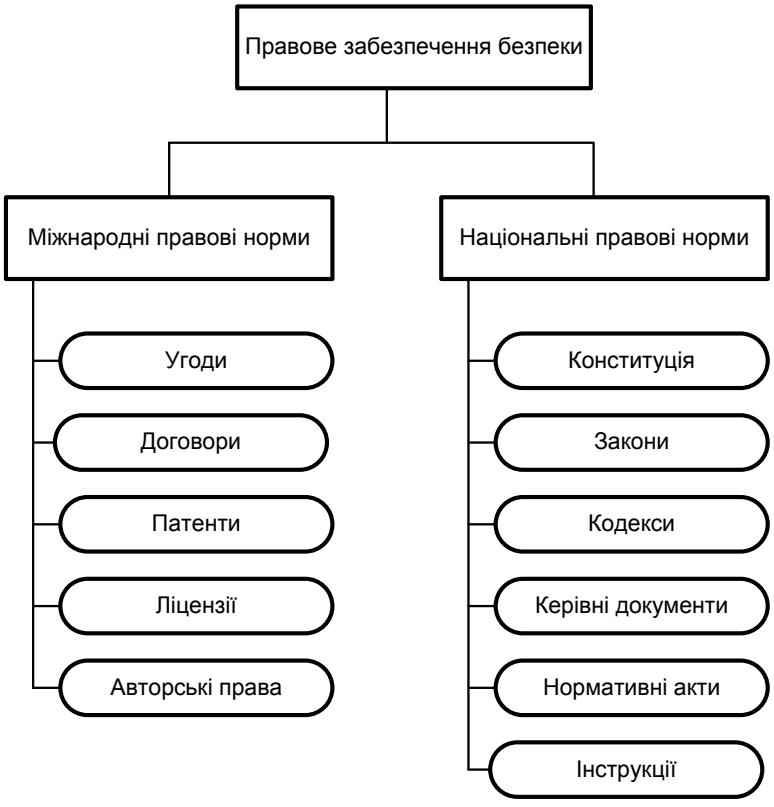

Рисунок 5.5 – Правове забезпечення безпеки інформації

програмістів, удосконалення карного і цивільного законодавства і судочинства. До них відносяться також питання суспільного контролю за розробниками комп’ютерних і прийняття відповідних міжнародних договорів про обмеження,

якщо вони впливають або можуть впливати на військові, економічні і соціальні аспекти країн. В останні роки в Україні з'явилися роботи з проблем правової боротьби з комп'ютерними злочинами і відповідно і вітчизняне законодавство стало на шлях боротьби з комп'ютерною злочинністю.

До організаційно-адміністративних заходів (рисунок 5.6) відносяться: охорона КС, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки одним спеціалістом, наявність плану відеовлення працездатності об'єкту (комп'ютерного центру) після виходу його з ладу, обслуговування ОЦ сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення його роботи, універсальність засобів захисту від усіх користувачів,

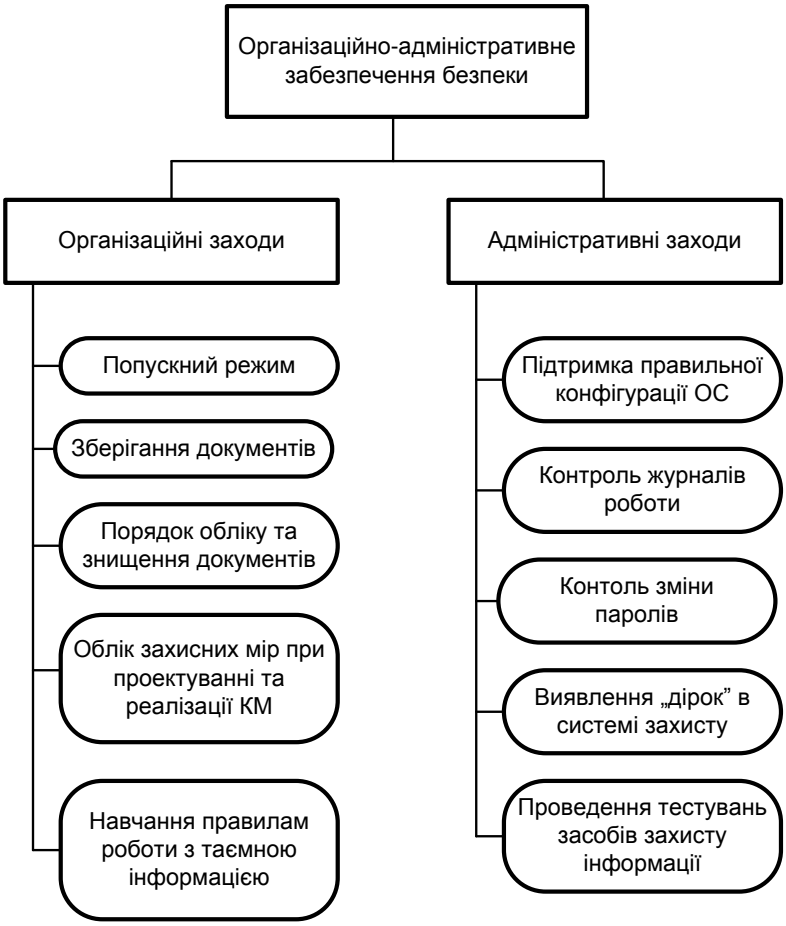

Рисунок 5.6 – Організаційно-адміністративні заходи захисту інформації в КМ

(включаючи вище керівництво), покладання відповідальності на осіб, які повинні забезпечувати безпеку ОЦ, вибір місця розташування ОЦ тощо.

До інженерно-технічних заходів, які подані на рисунку 2.7, можна віднести захист від несанкціонованого доступу до КС, резервування важливих комп'ютерних блоків і систем, резервне електроживлення, розробку та реалізацію спеціальних програмних і апаратних комплексі тощо.

Фізичні засоби містять у собі різні інженерні засоби, які перешкоджають

фізичному проникненню зловмисників на об’єкти захисту, які захищають персонал, матеріальні засоби і фінанси, інформацію про протиправні дії.

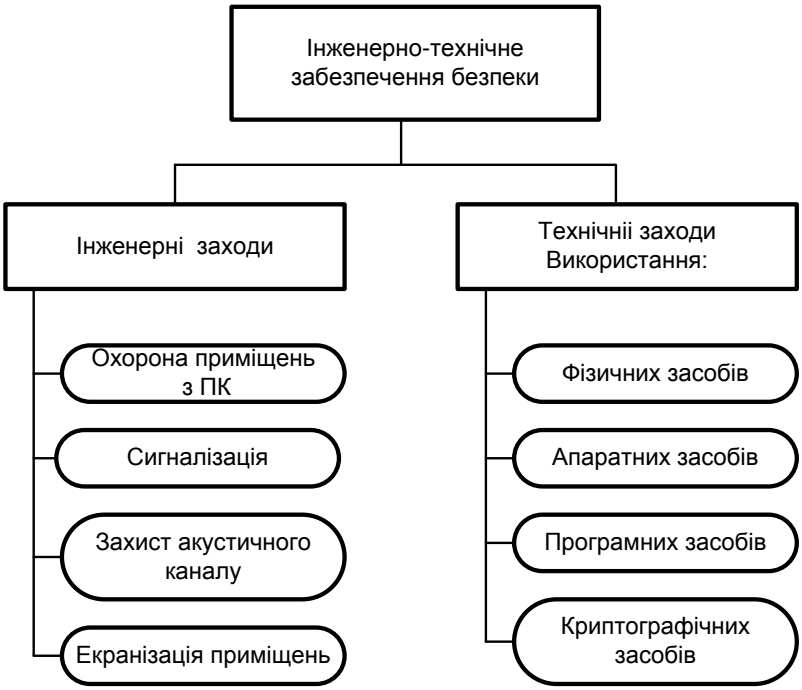

Рисунок 2.7 – Основні інженерно-технічні заходи захисту інформації

Програмні засоби – це спеціальні програми, програмні комплекси і системи захисту інформації в КС (інформаційних системах) різного призначення і засобах обробки даних.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, яка передана (передається) по каналах зв’язку, збереженої та опрацьованої на комп’ютерах з використанням методів шифрування.

ТЕМА 6. ЗАСОБИ, МЕТОДИ І СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

6.1. Засоби захисту інформації в комп’ютерних системах.
6.2. Методи і системи захисту інформації.
6.3. Методи ідентифікації і встановлення достовірності об’єктів і суб’єктів.

6.1. Засоби захисту інформації в комп’ютерних системах

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об’єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням комп'ютерів, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Правові засоби захисту - чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання. Перехід до інформаційного суспільства вимагає удосконалення використання ІТ.карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи, було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Вони охоплюють:

- заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);
- заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);
- заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.);
- розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є неодмінною частиною захисту інформації. Їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації, а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

Засоби фізичного (технічного) захисту інформації - це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

- засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;

- засоби захисту системи електроживлення. Американські дослідники з компанії Best Power після п’яти років досліджень проблем електроживлення зробили висновок: на кожному комп’ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності ІС можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;

- засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

- засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Розглядаючи програмні засоби захисту, доцільно спинитись на *стеганографічних методах*. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на друкуючих пристроях комп'ютерів компконтрактів з малопомітними викривленнями обрисів окремих символів тексту - так вносилась шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи:

1) додатковий захист - засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

2) вбудований захист - механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

6.2. Методи і системи захисту інформації

Функції і завдання захисту інформації визначають склад і структуру методів і систем захисту. Перелік основних методів захисту інформації поданий на рисунку 6.1. Одним із основних видів загроз цілісності і конфідеційності інформації, а також працездатності КС є навмисні загрози, реалізація яких заздалегідь планується зловмисником для нанесення шкоди. Даний суб'єктивізм безпосередньої реалізації можна розділити на дві групи:

- загрози, реалізація яких здійснюється при постійній участі людини (зловмисника);
- загрози, реалізація яких здійснюється відповідними комп'ютерними програмами без безпосередньої участі людини.

Завдання захисту від загроз кожного з цих типів однакові і полягають в наступному:

- унуможливення несанкціонованого доступу до ресурсів комп'ютерних систем;
- унеможливення несанкціонованого використання комп'ютерних ресурсів, якщо доступ до них все-таки здійснений;
- своєчасно виявити факт несанкціонованих дій і усунути причини, а також наслідки їх реалізації.

Способи вирішення перерахованих завдань захисту від несанкціованих дій з боку людей і комп'ютерних програм суттєво відрізняються один від одного.

Основні функції системи захисту полягають в тому, що перепони несанкціонованого доступу людей до ресурсів КС полягають перш за все в ідентифікації та підтвердженні достовірності користувачів при доступі в КС , а також розмежуванні їх доступу до комп'ютерних ресурсів.

Важливою є також функція коректного завершення сеансу роботи користувачів, що запобігає можливості реалізації загрози маскування під санкіонного користувача КС.

Захист інформації від дослідження і копіювання передбачає криптографічний захист даних, які захищаються, і виконується шляхом їх шифрування. Крім того, має бути передбачене знищення залишкової інформації, а також аварійне знищення даних.

Захист програм від копіювання запобігає можливості виконання несанкціоновано скопінованої програми на іншому комп'ютері. Захист програм від дослідження дозволяє захистити від дослідження алгоритмічні і інші деталі реалізації програми.

Системою захисту стосовно будь-якого користувача мають бути передбачені наступні етапи допуску до комп'ютерної (обчислювальної) системи:

- ідентифікація;
- встановлення достовірності (аутентифікація);
- визначення повноважень для подальшого контролю і розмежування доступу до комп'ютерних ресурсів.

Ці етапи повинні виконуватися і при підключенні до КС таких пристроїв, як віддалені робочі станції і термінали.

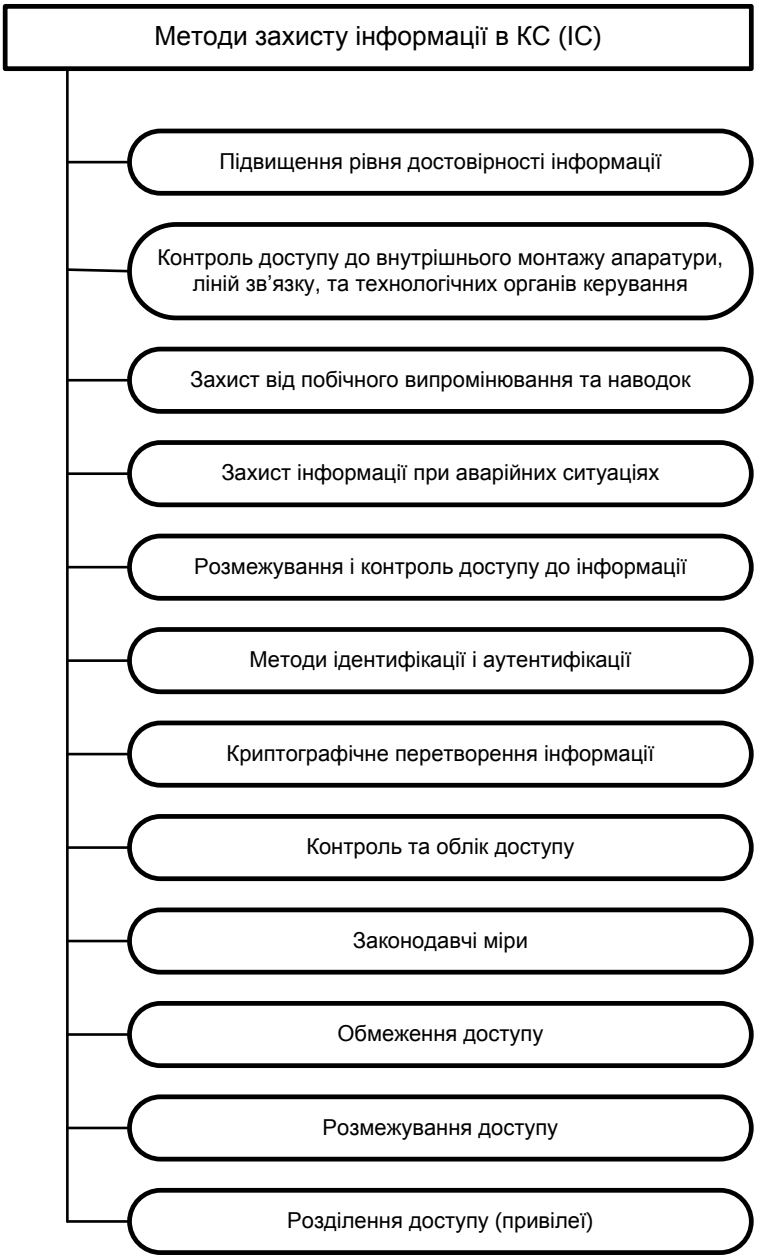

Рисунок 6.1 – Методи захисту інформації в КС (ІС)

6.3. Методи ідентифікації і встановлення достовірності об'єктів і суб'єктів

Ідентифікація необхідна для вказання КС унікального ідентифікатора користувача, який звертається до неї, з метою подальшого виконання захисних функцій.

Процес встановлення достовірності (аутентифікація) полягає в перевірці особи користувача, який намагається ввійти в систему.

Для особливо надійного розпізнавання застосовуються методи, які ґрунтуються на використанні технічних засобів визначення суто індивідуальних характеристик людини (голосу, відбитків пальців, структури зіниці ока) тощо.

На міру інформаційної безпеки при використанні простого парольного

методу перевірки достовірності користувачів великий вплив роблять обмеження на мінімальний і максимальний час дійсності кожного пароля. Чим частіше змінюється пароль, тим більша безпека.

Існують багато методів, які використовуються для ідентифікації і встановлення достовірності різноманітних об’єктів, які згруповані, як показано на рисунку 6.2.

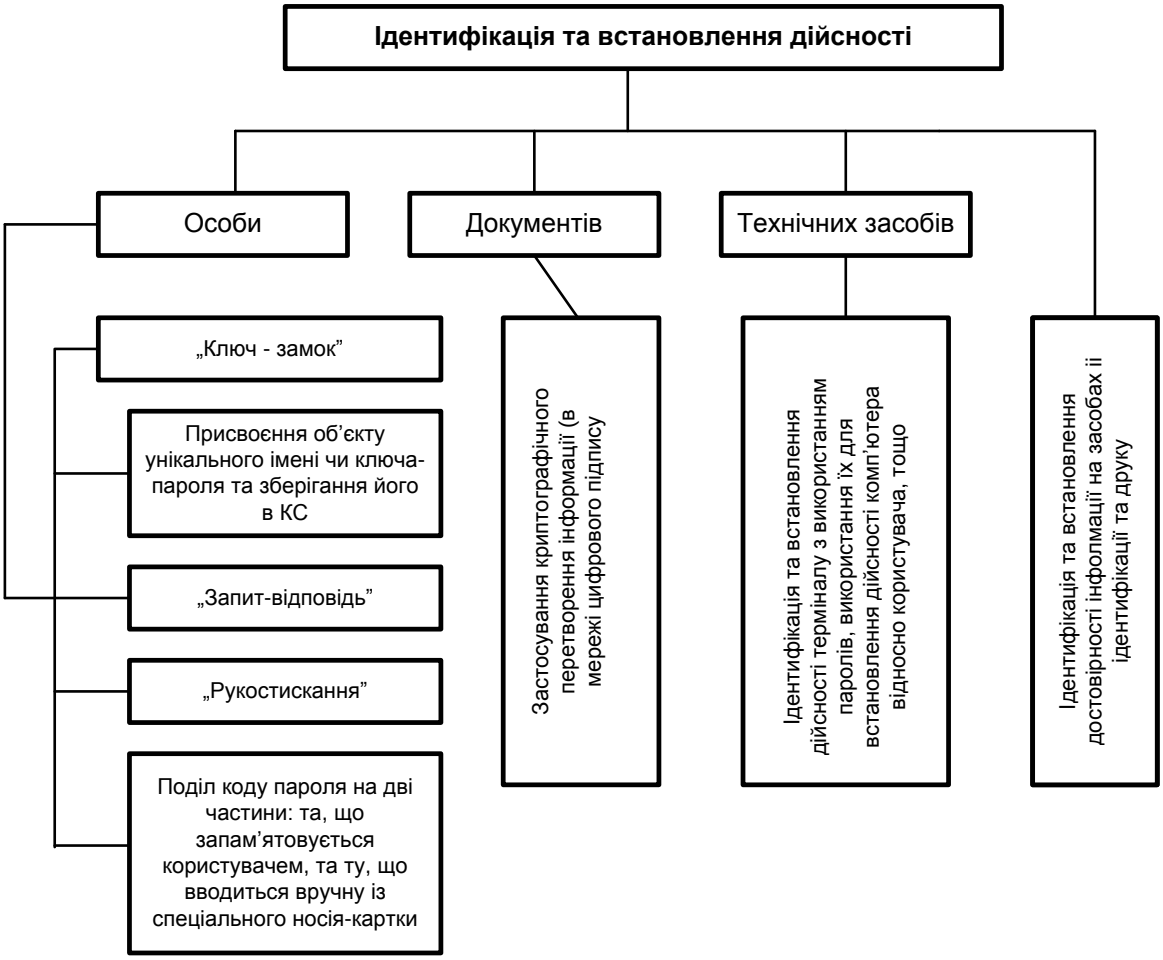

Рисунок 6.2 – Методи, які використовуються для втановлення дійсності об’єктів захисту інформації в КС

При обміні інформацією в будь-якому випадку рекомендується передбачити взаємну перевірку достовірності повноважень об’єкту та суб’єкта. Якщо обмін здійснюється за допомогою мережі, то ця процедура повинна виконуватися обов’язково.

Метод «запит-відповідь». При використанні цього методу у КС завчасно створюється і особливо захищається масив запитань, який включає як запитання загального характеру, так і персональні запитання, що стусуються конкретного користувача. Для підтвердження достовірності користувача система послідовно ставить йому низку випадково обраних запитань, на які він повинен дати відповідь. Розпізнавання вважається позитивним, якщо користувач правильно відповів на всі запитання.

Метод односторонніх функцій. Односторонні функції широко використовуються в асиметричних криптосистемах і мають наступну властивість: при заданому значенні x відносно легко обчислити значення функції $f(x)$, однак якщо відомо значення $y = f(x)$, то не існує простого способу обчислення значення x.

Згідно *методу «рукостискання»* існує функція F, яка відома лише користувачеві і КС. При вході користувача у КС системою захисту генерується випадкове число або випадкова послідовність символів X і обчислюється функція $F(X)$ для даного користувача. Далі X виводиться користувачеві, який повинен обчислити $F(X)$ і ввести її значення в систему. Ці значення порівнюються системою, і якщо вони співпадають, то користувач отримує доступ до КС.

Ідентифікіція і встановлення достовірності технічних засобів. В даному випадку широко використовуються паролі як для ідентифікації і встановлення достовірності терміналу, з якого користувач входить в систему, так і для зворотного встановлення достовірності комп'ютером користувача.

Ідентифікація і встановлення достовірності документів. Достовірність документів необхідно розглядати з наступних позицій:

- документ сформова ний безпосередньо в даній КС;
- документ сформований з віддалених об'єктів.

В першому випадку достовірність документа гарантується засобами захисту інформації і використанням криптографічного перетворення інформації. Інформація закривається кодом пароля.

У другому випадку також використовується методи криптографічного перетворення інформації, якщо документи відносно довго зберігалися в пам'яті КС, або ж транспортувалися територією, яка не охоронялася.

Ідентифікація і встановлення достовірності інформації на засобах її відображення ідруку. Всі міркування стосовно методів визначення достовірності документів також належать і до методів встановлення достовірності інформації, яка міститься на засобах її відображення.

Своєчасне виявлення несанкціонованих дій користувачів. Своєчасне виявлення несанкціонованих дій користувачівгрунтується на виконанні наступних функцій:

- періодичний контроль цілісності інформації;
- контроль правильності функціонування системи захисту;
- реєстрація і сигналізація.

ТЕМА 7. ЗАХИСТ ІНФОРМАЦІЇ В ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ

7.1. Особливості захисту інформації в ПК.
7.2. Загрози інформації в ПК.
7.3. Захист ПК від несанкціонованого доступу.

7.1. Особливості захисту інформації в ПК

Персональні комп'ютери (ПК) володіють всіма властивостями комп'ютерів інших класів, тому, взагалі кажучи, всі проблеми захисту інформації в

побудованих на їх ґрунті системах і підходи до захисту аналогічні розглянутим вище. Проте персональним комп'ютерам властивий ряд таких властивостей, які, з одного боку сприяють захисту, а з іншої - ускладнюють його.

Особливості ПК з точки зору захисту інформації є наступними:

- малі габарити і вага, що робить їх не просто транспортабельними, а переносними - особливо це стосується ноутбуків;
- наявність жорсткого диска великого об'єму, що зберігає записані дані після вимкнення живлення;
- наявність можливості відключення змінних запам'ятовуючих пристроїв (флеш-карт) великого об'єму і малих габаритів;
- можливість роботи в дротових та бездротових мережах;
- оснащеність програмним забезпеченням з широкими функціональними можливостями;
- масовість виробництва і поширення;
- мала вартість.

Для ПК питання загальної організації захисту можуть бути вирішені:

- фізичною ізоляцією (наприклад, розміщенням ПК в окремій кімнаті , яка закривається на ключ), тому переважаючу роль відіграє внутрішній захист;
- турботу про захист інформації повинні виявляти самі користувачі, які не лише не є фахівцями в області захисту, але в багатьох випадках взагалі мають лише навички безпосереднього вирішення обмеженого кола задач.

На формування множини можливих підходів до захисту інформації в ПК і вибір найбільш доцільного з них в конкретних ситуаціях виначальний вплив виявляють наступні чинники:

- цілі захисту;
- потенційно можливі способи захисту;
- наявні засоби захисту.

Основними цілями захисту інформації в ПК є традиційні:

- забезпечення фізичної цілісності;
- забезпечення логічної цілісності;
- попередження несанкціонованого отримання інформації;
- попередження несанкціонованої модифікації інформації;
- попередження несанкціонованого копіювання інформації.

Забезпечення логічної цілісності інформації для ПК малоактуально, інші ж цілі стосовно ПК можуть бути конкретизовані наступним чином.

Забезпечення фізичної цілісності. Фізична цілісність інформації в ПК залежить від цілісності самого ПК, цілісності дисків і пристроїв флеш-пам'яті, цілісності інформації на дисках, флеш-пам'яті і в оперативний пам'яті. У широкому спектрі загроз цілісності інформації в ПК слід звернути особливу увагу на загрози пов'язані з недостатньо високою кваліфікацією значного числа власників ПК. У цьому плані особливо небезпечним є знищення або спотворення даних на жорсткому диску (HDD), на якому безпосередньо користувачем можуть накопичуватися дуже значні об'єми інформації.

Попередження несанкціонованої модифікації. Небезпечним різновидом несанкціонованої модифікації інформації в ПК є дія шкідливих програм, які

можуть руйнувати або знищувати програми чи масиви інформації (даних). Дана небезпека набуває актуальності у зв'язку з тим, що серед власників ПК є практика обміну CD та DVD-дисками, автономними жорсткими дисками та пристроями флеш-пам'яті.

Попередження несанкціонованого отримання інформації, яка знаходить в ПК. Це особливо актуально втих випадках, коли інформація, яка зберігається або опрацьовується, містить службову інформацію для обмеженого кола осіб, або інформацію, яка відноситься до безпеки держави.

7.2. Загрози інформації в ПК

Специфічні особливості архітектурної побудови і способів використання ПК дозволяють конкретизувати значну частину загроз (каналів витоку) інформації. Характерні для ПК канали прийнято класифікувати за типом засобів, які використовуються з метою несанкціонованого отримання інформації, і виділяють три типи засобів**:** *людина, апаратура, програма*.

Групу каналів, в яких основним засобом несанкціонованого отримання інформації є людина, складають:

- носії інформації (магнітних дисків, роздруків і т. ін.);
- зчитування або фотографування інформації з екрану;
- зчитування або фотографування інформації з оригіналів роздруківок.

У групі каналів, основним засобом використання яких служить апаратура, виділяють:

- підключення до пристроїв ПК спеціальної апаратури, за допомогою якої можна знищувати або копіювати інформацію, яка захищається;
- реєстрацію за допомогою спеціальних засобів електромагнітних випромінювань пристроїв ПК в процесі опрацювання інформації, яка захищається.

Нарешті, третю групу каналів (основний засіб використання яких - програми) утворюють:

- програмний несанкціонований доступ до інформації;
- знищення (спотворення) або копіювання інформації, що захищається, за допомогою програмних закладок або пасток;
- зчитування залишкової інформації з ОЗП;
- програмне копіювання інформації з магнітних носіїв.

Повний базовий перелік тих модулів і блоків, в яких можуть знаходитися дані, які підлягають захисту, є наступним:

- системні плати ПК;
- зовнішні жорсті диски та пристрої флеш-пам'яті;
- жорсткі диски всередині ПК;
- монітор;
- друкуючий пристрій;
- канали сполучення.

Захисту підлягають дані, що знаходяться в кожному з перерахованих місць.

7.3. Захист ПК від несанкціонованого доступу

Як показує практика, несанкціонований доступ є однією з найсерйозніших загроз для зловмисного заволодіння інформацією, що захищається, в сучасних КС. Для ПК небезпека цієї загрози в порівнянні з великими комп'ютерами збільшується, чому сприяють наступні об'єктивно існуючі обставини:

- переважна частина ПК розташовується безпосередньо в робочих кімнатах фахівців, що створює сприятливі умови для доступу до них сторонніх осіб;
- багато ПК служать колективним засобом опрацювання інформації, що знеособлює відповідальність, у тому числі і за захист інформації;
- сучасні ПК оснащені накопичувачами на жорстких дисках дуже великої ємності;
- зовнішні накопичувачі виробляються в такій масовій кількості, що вже давно використовуються для поширення інформації так само, як і паперові носії;
- спочатку ПК створювалися саме як персональний засіб автоматизації опрацьовання інформації, а тому і не оснащувалися спеціально засобами захисту від несанкціонованого доступу.

Основними механізмами захисту ПК від несанкціонованого доступу є наступні:

- фізичний захист ПК і носіїв інформації;
- розпізнавання (аутентифікація) користувачів та компонентів інформації;
- розмежування доступу до елементів інформації;
- криптографічний захист інформації, яка зберігається на насіях;
- криптографічний захист інформації в процесі її опрацювання;
- реєстрація всіх звернень до інформації, що захищається.

Аутентифікація (розпізнавання) користувачів в ПК не має принципових відмінностей від тих способів, що вже були розглянуті.

Для *розпізнавання компонентів опрацювання даних,* тобто ПК, ОС, програм функціонального опрацювання, масивів даних (таке розпізнавання особливо актуальне при роботі в комп'ютерній мережі), використовуються наступні засоби:

- спеціальні апаратні блоки-приставки (для розпізнавання комп'ютера, терміналів, зовнішніх пристроїв);
- спеціальні программи, що реалізують процедуру «запит-відповідь»;
- контрольні суми (для розпізнавання програм і масивів даних).

Розпізнавання за допомогою блоків-приставок полягає в тому, що технічні засоби оснащуються спеціальними пристроями, які генерують спеціальні індивідуальні сигнали. З метою попередження перехоплення цих сигналів і подальшого їх використання, вони можуть передаватися в зашифрованому вигляді, причому періодично може змінюватися не лише ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення.

Розпізнавання за контрольною сумою полягає в тому, що для програм і масивів даних завчасно обчислюються їх контрольні суми (або інші величини, залежні від змісту ідентифікованих об’єктів).

Захист від комп'ютерних вірусів та інших програмних дій є окремим напрямком захисту процесів опрацювання інформації в ПК, комп'ютерних та інформаційних системах і був розглянутий вище.

ТЕМА 8. ОСНОВИ КРИПТОГАФІЇ ТА КРИПТОАНАЛІЗУ

8.1. Основні положення та визначення криптографії.
8.2. Симетричні, асиметричні та комбіновані криптосистеми.

8.1. Основні положення та визначення криптографії

Завдання захисту інформації в комп'ютерних системах перетворюється сьогодні в одну з найактуальніших внаслідок широкої розповсюдженості 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 вважається широке впровадження в 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 з 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, спрямованих на приховування змісту переданої або збереженої інформації. І хоча на цей час сфера застосування криптографічних механізмів значно розширилася, основні ідеї можна проілюструвати саме на прикладі забезпечення 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 погляд відбивав таку точку зору: 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

криптоаналітични-ми методами, а відповідну галузь досліджень – криптоаналізом. Отже, криптоаналіз – це наука, спрямована на подолання криптографічного захисту.

На сьогоднішній день 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 є шифруванням. 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 (дешифруванням), 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.

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

8.2. Симетричні, асиметричні та комбіновані криптосистеми

У процесі шифрування використовується певний алгоритм шифрування (рисунок 8.1), на вхід якому подаються незашифроване повідомлення (англійською – plaintext) і ключ шифрування. Виходом алгоритму є зашифро-

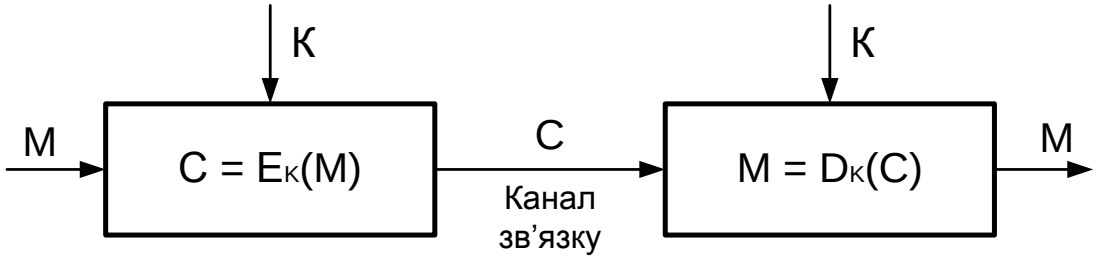

Рисунок 8.1 - Загальна структурна схема симетричного шифрування

ване повідомлення, що називається англійською ciphertext (шифро-текст). 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 вико-

ристовувався при шифруванні, або ключа, який можна легко одержати з ключа шифрування.

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

Наглядно схему симетричного шифрування інформації приведено на рисунку 8.2

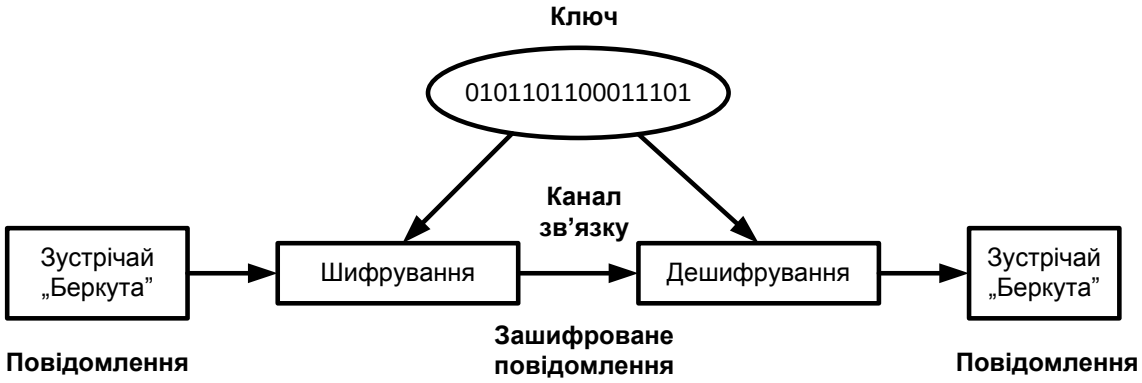

Рисунок 8.2 – Схема симетричного шифрування

Стійкість, яку забезпечує традиційна криптографія, залежить від кількох факторів.

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.

Клод Шеннон увів 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.

Симетричні криптоалгоритми

Алгоритми симетричного шифрування відрізняються способом, яким обробляється вихідний текст.

Симетричні алгоритми шифрування поділяються на:

- потокові;
- блокові.

Алгоритми, в яких відкритий текст обробляється побітно, називаються *потоковими алгоритмами* або *потоковими шифрами.* В інших алгоритмах відкритий текст розбивається на блоки, які складаються з декількох біт. Такі алгоритми називаються *блоковими* або *блоковими шифрами*.

В симетричних блокових алгоритмах блок тексту розглядається як додатне ціле число, або як кілька незалежних додатних цілих чисел. Довжина блоку завжди дорівнює 2^n.

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);
- операція додавання за модулем 2^{32} або за модулем 2^{16};
- 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 проце-сорі з мінімальними вимогами до пам'яті;
- використовувати заздалегідь обчислені підключі. При неможливості попереднього обчислення підключів можливе лише зменшення швид-кодії. Завжди повинна бути можливість шифрування даних без яких-небудь попередніх обчислень.

Складатися зі змінного числа ітерацій. Для застосувань з малень-кою 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 поданий у вигляді, наведеним на рисунку 8.3.

Асиметричні криптоалгоритми

У симетричних криптоалгоритмах 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.

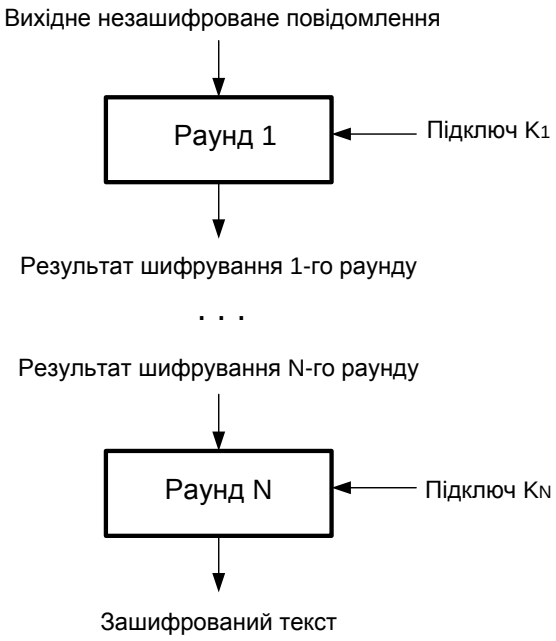

Рисунок 8.3 - Структура симетричного алгоритму

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

Суть таких систем полягає в тому, що кожним суб'єктом інформаційного обміну генеруються два ключі (рисунок 8.4), які 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. Секретний 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). Розшифрувати повідомлення можливо лише на відповідному

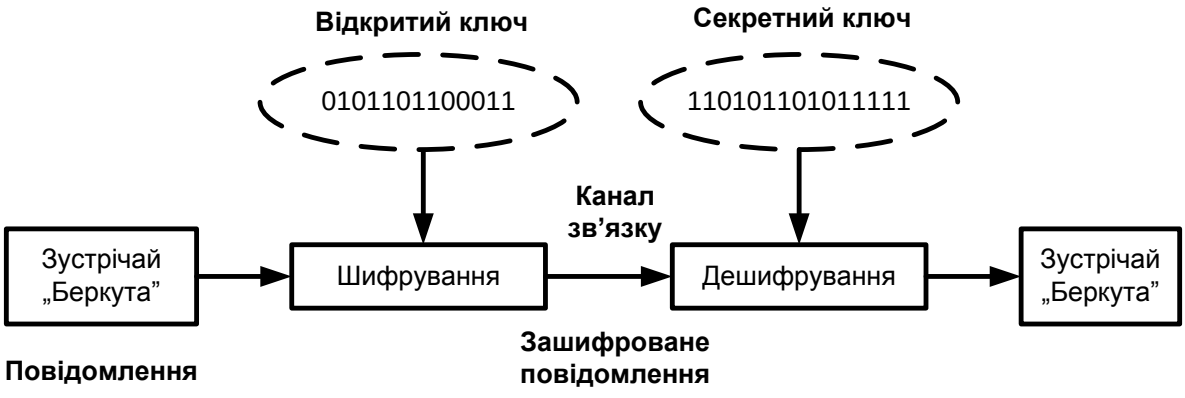

Рисунок 8.4 – Схема несиметричного (асиметричного) шифрування

приватному ключі, відомому лише безпосередньо адресату.

Асиметричні криптосистеми використовують так звані односторонні функції, які мають наступну властивість: при заданому значенні x відносно легко обчислити значення функції $f(x)$, однак якщо відомо значення $y = f(x)$, то не існує простого способу обчислення значення x.

Велика кількість класів незворотних функцій і породжує всю різноманітність криптосистем з відкритим ключем. Однак в самому означенні є деяка невизначеність: «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 (секретного) 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:

1) як самостійні засоби захисту інформації;
2) як засоби автентифікації користувачів;
3) як засоби розповсюдження ключів.

В 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.

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 і недоліки:

- генерація нових секретних і відкритих ключів заснована на генерації нових великих простих чисел, а перевірка простоти чисел займає багато бчислювального часу;
- процедури шифрування і розшифрування, пов’язані зі зведенням у степінь багатозначного числа, досить громіздкі.

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

Комбінований метод шифрування

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. Симетрична криптосистема застосовується для шифрування і передачі вихідного відкритого тексту. У результаті криптосистема з відкритим ключем не замінює 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 такий.

1. Створення (наприклад, згенерувати випадковим чином) симетричного ключа, названого у даному методі сеансовим ключем Ks.

2. Шифрування повідомлення М на сеансовому ключі Ks.

3. Шифрування сеансового ключа Ks на відкритому ключі K_B користувача В.

4. Передача відкритим каналом зв'язку на адресу користувача В зашифрованого 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 Ks.

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

При використанні комбінованого методу шифрування можна бути впевненим у тому, що тільки користувач В зможе правильно розшифрувати ключ Ks 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 криптоистеми слід здійснювати таким чином, щоб зловмиснику було однаково важко атакувати будь-який механізм захисту комбінованої криптосистеми. У таблиці 8.1 наведено розповсюджені довжини ключів симетричних і асиметричних криптосистем, для яких труднощі атаки повного перебору приблизно дорівнюють труднощам факторизації відповідних модулів асиметричних криптосистем.

Таблиця 8.1 – Довжини ключів для симетричних і асиметричних криптосистем

Довжина ключа симетричної криптосистеми, біт	Довжина ключа асиметричної криптосистеми, біт
56	384
64	512
80	768
112	1 792
128	2 304

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 K_A 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.

Комбінований метод шифрування є найбільш раціональним, поєднуючи в собі високу швидкодію симетричного шифрування та високу криптостійкість, яка гарантується системами з відкритим ключем.

ТЕМА 9. КЛАСИФІКАЦІЯ КРИПТОАЛГОРИТМІВ

9.1. Тайнопис, криптографія з ключем.
9.2. Симетричні та асиметричні криптоалгоритми.

9.1. Тайнопис, криптографія з ключем

Тайнопис - спеціальна система зміни звичайного листа, зрозуміла лише вузькому колу осіб чи одній особі. Синонімом слова «тайнопис» є слово «криптографія».

Криптографія - (від грець. kryptós - прихований і gráphein - писати) - наука про математичні методи забезпечення конфіденційності і автентичності інформації.

Тривалий час під криптографією розуміли лише шифрування - процес перетворення звичайної інформації у незрозумілий шифротекст.

Таємна передача повідомлень, непомітна для навколишніх необізнаних осіб, існує з давніх часів. Прикладом може служити мова жестів, широко використовувана фокусниками і картковими шулерами. За допомогою таких таємних жестів асистент підказує фокусникові під час сеансу на очах у глядачів, а пара шулерів підказують один одному ходи під час гри на очах нічого непідозрюючих партнерів.

Екзотичний метод використовувався американцями під час другої світової війни: кораблі ВМФ США здійснювали зв'язок на мові нечисленного і компактно проживаючого індіанського племені. На кожному кораблі було декілька індіанців-«шифрувальників», а у супротивника не було практично жодних шансів здобути такого «криптографа».

З виникненням писемності завдання забезпечення секретності і достовірності передаваних повідомлень стало особливо важливим. Адже повідомлення, передане словесно або показане жестами, доступно для стороннього тільки у момент передачі, а в його авторстві і достовірності у одержувача ніяких сумнівів не виникає, тому що він бачить свого співбесідника.

Коли ж повідомлення записане на папері, воно вже живе окремим життям і існує у матеріальному світі набагато триваліший проміжок часу. І у людей, охочих ознайомитися з його змістом проти волі відправника і одержувача,

з'являється значно більше можливостей зробити це. Тому після виникнення писемності з'явилося мистецтво тайнопису, мистецтво «таємно писати» - набір методів, призначених для секретної передачі записаних повідомлень від однієї людини іншій.

Криптографія у минулому використовувалася переважно у військових цілях. Проте зараз, із становленням інформаційного суспільства, вона стає центральним інструментом для забезпечення конфіденційності.

Криптографія займається всіма видами секретного обміну повідомленнями, включаючи таємне листування, аутентифікацію (встановлення достовірності, від грець. authentikos - справжній), цифрові підписи, електронні гроші і багато чого іншого.

Криптографія - це наука про те, як забезпечити секретність повідомлення, а криптоаналіз - це наука про те, як розкрити шифроване повідомлення, тобто як витягувати відкритий текст повідомлення. Криптографією займаються криптографи, а криптоаналізом займаються криптоаналітики.

Суть шифрування - не приховувати сам факт передачі повідомлення, але зробити його недоступним стороннім. Для цього повідомлення має бути записане так, щоб з його вмістом не міг ознайомитися ніхто, за винятком самих кореспондентів. Шифрування є перетворенням повідомлення по певних правилах, що робить його безглуздим набором знаків для необізнаної в таємницю шифру людини.

Коли об'єми, що підлягали закриттю інформації стали критичними, на допомогу людям були створені складніші механічні пристрої для шифрування, наприклад, німецька шифрувальна машина Енігма. Англійським криптоаналітикам вдалося зламати німецькі коди, внаслідок чого вони могли читати німецькі секретні депеші.

Основними споживачами криптографічних послуг були дипломатичні і шпигунські місії, таємні канцелярії правителів і штаби військових з'єднань і флотів і т. п..

З виникненням комп'ютерів і проникненням їх в різні сфери життя виникла принципово нова галузь господарства - інформаційна індустрія. Після розповсюдження комп'ютерів в діловій сфері практична криптографія зробила в своєму розвитку величезний стрибок:

- були розроблені стійкі шифри з ключами (відкритим і секретним), призначені для забезпечення секретності і цілісності передаваних або таких, що зберігаються даних;
- були створені методи вирішення нових, нетрадиційних завдань сфери захисту інформації.

Ключ - це секретна інформація, яка використовується криптографічним алгоритмом при шифруванні / розшифровці повідомлень, постановці і перевірці цифрового підпису, обчисленні кодів автентичності (MAC).

При використанні одного і того ж алгоритму результат шифрування залежить від ключа. Для сучасних алгоритмів сильної криптографії втрата ключа призводить до практичної неможливості розшифрувати інформацію.

Криптографічні ключі розрізняються згідно алгоритмів, в яких вони використовуються.

Секретні (симетричні) ключі - ключі, що використовуються в симетричних алгоритмах (шифрування, вироблення кодів автентичності). Головна властивість симетричних ключів – використання їх для виконання як прямого, так і зворотного криптографічного перетворення (шифрування / розшифрування, обчислення MAC / перевірка MAC).

Асиметричні ключі - ключі, що використовуються в асиметричних алгоритмах (шифрування, ЕЦП). Більш точно, вони є ключовою парою, оскільки складаються з двох ключів:

Закритий ключ (англ: Private key) - ключ, відомий тільки своєму власнику. Тільки збереження користувачем в таємниці свого закритого ключа гарантує неможливість підробки зловмисником документа, котрий завіряє цифровий підпис.

Відкритий ключ (англ: Public key) - ключ, який може бути опублікований і використовується для перевірки достовірності підписаного документа, а також для попередження шахрайства з боку завіряючої особи у випадку відмови її від підпису документу. Відкритий ключ підпису обчислюється як значення деякої функції від закритого ключа, але знання відкритого ключа не дає можливості визначити закритий ключ.

За допомогою секретного ключа легко обчислюється відкритий ключ, але за відомим відкритим ключом практично неможливо обчислити секретний. В алгоритмах ЕЦП підпис зазвичай ставиться на секретному ключі користувача, а перевіряється на відкритому. Таким чином, будь-хто може перевірити, чи дійсно даний користувач поставив даний підпис.

9.2. Симетричні та асиметричні криптоалгоритми

DES (Data Encryption Standard) – стандарт шифрування даних

Найпоширенішим і найбільш відомим алгоритмом симетричного шифрування є DES (Data Encryption Standard – стандарт шифрування даних). Алгоритм був розроблений у 1977 році, в 1980 році був прийнятий NIST (National Institute of Standards and Technolody США) у якості стандарту (FIPS PUB 46).

DES є класичною сіткою Фейстеля з двома множинами (рисунок 9.1).

Дані шифруються 64-бітними блоками з використанням 56-бітного ключа. До секретних 56 бітів додається 8 бітів парності, тобто загальна довжина ключа дорівнює 64 біти.

Процес шифрування складається із чотирьох етапів. На першому з них виконується початкова перестановка (IP) 64-бітного вихідного тексту (забілювання), під час якої біти перемішуються відповідно до стандартної таблиці. Наступний етап складається з 16 раундів однієї й тієї ж функції, яка використовує операції зсуву і підстановки. На третьому етапі ліва і права половини виходу останньої (16-ї) ітерації міняються місцями. Нарешті на четвертому етапі виконується перестановка IP^{-1} результату, отриманого на третьому етапі. Перестановка IP^{-1} обернена до початкової перестановки IP.

Процес шифрування полягає в початковій перестановці бітів 64-бітового блоку, шістнадцяти циклах шифрування і, нарешті, зворотної перестановки бітів (рисунок 9.2).

Процес розшифрування в DES є операцією зворотною шифруванню і виконується шляхом повторення операцій шифрування в зворотній послідовності. На вхід алгоритму подається зашифрований текст, але ключі Ki використовуються в оберненій послідовності: K16 використовується на першому

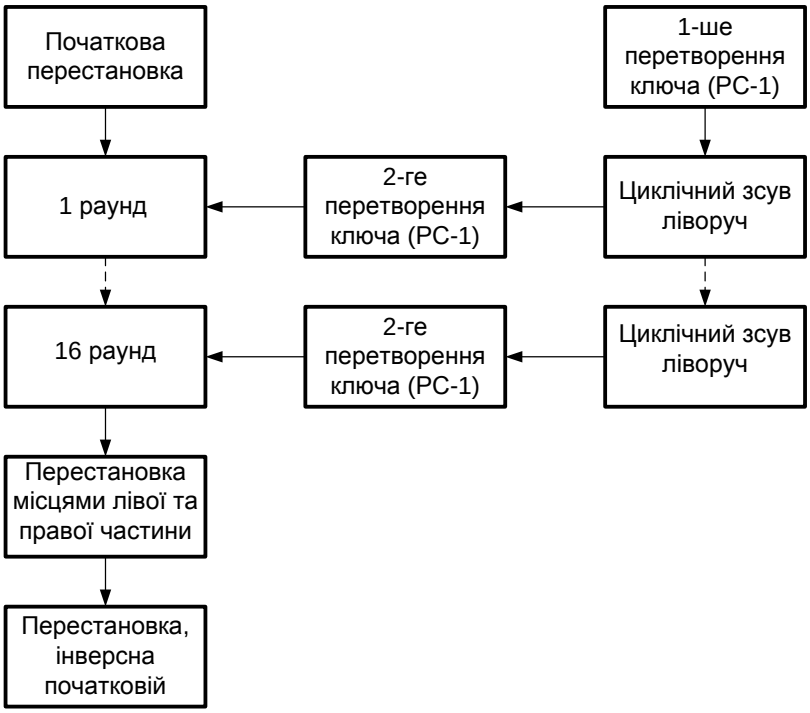

Рисунок 9.1 - Загальна схема DES

раунді, K1 – на останньому раунді. Виходом цієї стадії є незашифрований текст.

Для створення «Власного алгоритму шифрування» можна скористатися програмою DISKREET з пакету Norton Utilities, яка призначена для зашифровування розділів на диску з застосуванням саме алгоритму DES. «Власний алгоритм шифрування» відрізняється від DES тільки числом ітерацій при шифруванні.

Через те, що довжина ключа рівна 56 бітам, існує 256 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.

Перевагами DES криптосистеми вважаються: 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 на сьогодні вважають: невелику довжину ключа, усього 56 біт. При сучасному рівні розвитку комп'ютерних засобів така довжина ключа не може забезпечувати потрібний рівень захисту для деяких типів інформації; наявність "слабких" ключів, викликана тим, що для генерування ключової послідовності виконується два незалежних регістри зсуву. Прик- ладом слабкого ключа може служити 1F1F1F1F0E0E0E0E. При цьому результатом генерування будуть ключові послідовності, однакові з вихідним ключем, в усіх 16 раундах. Існують також різновиди слабких ключів, що дають усього чотири

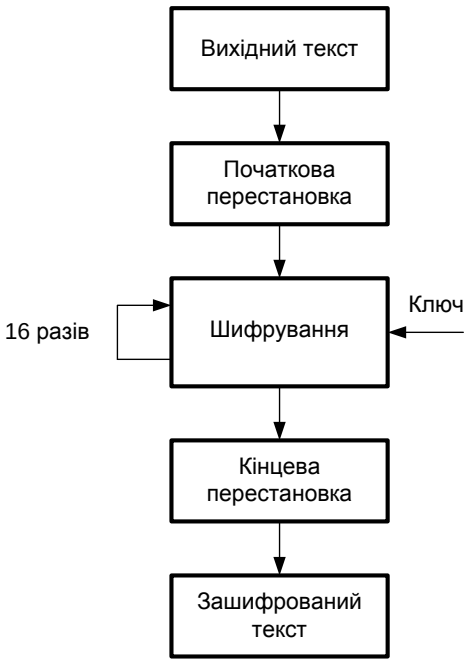

Рисунок 9.2 - Узагальнена схема шифрування в алгоритмі DES

ключові послідовності та «зв'язані» ключі, які отримуються один з одного інверсією одного біта; надмірність ключа, що має біти контролю парності. Наявність бітів контролю парності дозволяє відновити ключ при втраті його частини внаслідок збоїв комірок пам'яті.

Основним недоліком алгоритму DES є мала довжина ключа. Аналітики на це звертали увагу одразу після опублікування стандарту по тій причині, що не існувало таких комп'ютерних потужностей, які дозволили б реалізувати атаку «грубою силою», тобто повного перебору ключів. Після появи потужних комп'ютерів (комп'ютер DES-cracker) вдалося здійснити таку атаку за три дні, що 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 значно підсилюють стійкість алгоритму до атаки повного перебору ключів.

Потрійний *DES*

Існує багато різних варіантів потрійного DES. Найбільш популярними з 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(3DES EDE2)

У цьому алгоритмі використовується два ключі по 56 біт, тобто загальна довжина ключа дорівнює 112 біт. Шифрування даним алгоритмом передбачає етапи, які показані на рисунку 9.3. Як видно з рисунку, відкрите повідомлення M спочатку шифрується звичайним однократним DES на ключі K_1, потім розши-

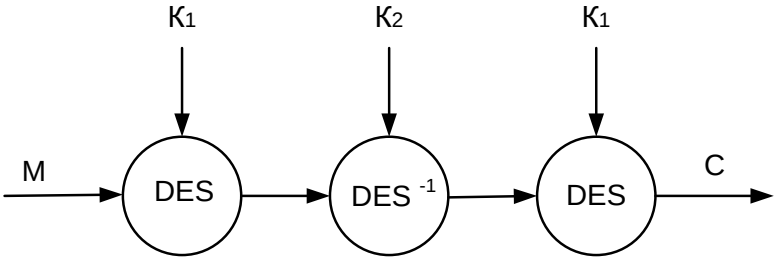

Рисунок 9.3 – Схема шифрування алгоритму 3DES EDE2

фровується на ключі K_2, після чого знов шифрується на K_1. У цьому випадку зростання криптостійкості досягається як збільшенням довжини загального ключа (до 112 біт + біти парності), так і кількістю 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 85 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 (3DES EDE3)

Відмінність від попереднього алгоритму полягає в тому, що тут використовується три ключі шифрування, отже, стійкість системи до атаки "грубою силою" ще зростає. Загальна довжина ключа досягає 56x3=168 біт + біти парності. У випадку K1 = K2= K3 3DES EDE3 перетворюється в однократний DES, який є в три рази повільнішим.

Шифрування за допомогою алгоритму 3DES EDE3 показано на рисунку 9.4.

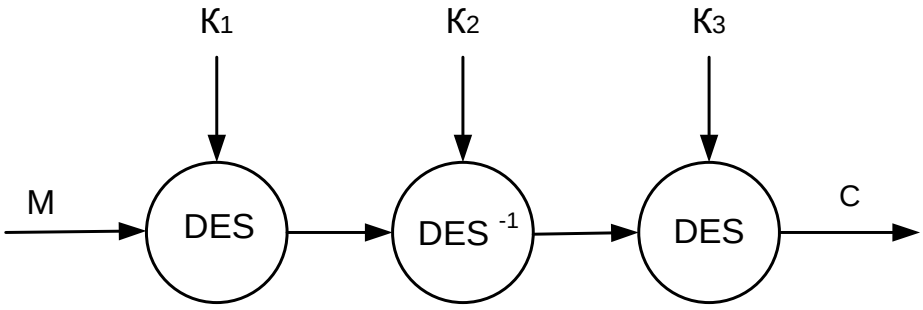

Рисунок 9.4 – Схема шифрування потрійним DES з трьома ключами

Розшифрування виконується аналогічно у зворотному порядку: спочатку шифроване повідомлення розшифровується на ключі $К_3$, потім зашифровується на ключі $К_2$, і, врешті решт, знов розшифровується, але на ключі $К_1$. Падіння швидкодії при роботі 3DES іноді дуже помітне, і, наприк лад, у режимі зчеплення блоків це сповільнення не вдається компен- сувати додатковим апаратним обладнанням. У багатьох випадках, наприклад, при шифруванні критичних каналів зв'язку, таке падіння продуктивності неприпустиме.

Алгоритм *DESX*

Цей алгоритм запропонований до застосування як модифікацію DES, який отримав назву *DESX (DES eXtended)*, і був вільний від недоліків *3DES*.

DESX визначається як $DESX_{K1,K2,K3} = K_2 \oplus DES_K(K_1 \oplus M)$. Як видно з наведеної формули, повний ключ DESX складається з трьох: першого зашумлюючого K_1, який додається за правилами XOR до відкритого повідомлення; ключа DES_K; другого зашумлюючого ключа K_2, який додається за XOR до результатів шифрування DES. Таким чином, загальна довжина ключа DESX становить 56 + 64 + 64 = 184 біти, що навіть більше, ніж у 3DES.

Що стосується збільшення часу обробки, то він усього на дві операції додавання за модулем 2 більший за звичайний DES.

Суттєвим для DESX є те, що цих дві операції XOR роблять шифр менш вразливим до атаки «грубою силою», проти чого і була спрямована дана розробка. DESX, однак, збільшує й стійкість простого DES проти диференціального та лінійного криптоаналізу, збільшуючи потрібну кількість проб з обраним відкритим текстом до 260.

Таким чином, практично з усіх боків DESX кращий за DES. Це простий алгоритм, сумісний з DES, ефективно реалізується апаратно, може використовувати існуюче апаратне забезпечення DES.

Крім вище приведених, розроблено і ряд інших симетричних крипто-алгоритмів (алгоритм криптографічного перетворення ГОСТ 28147-89, алгоритм Rijndael, криптоалгоритми RC2, RC5, IDEA та ін.).

У кінці 2000 р. Департамент спецзв'язку та захисту інформації СБУ та Інститут кібернетики імені В. Глушкова оголосили відкритий конкурс симетричних криптоалгоритмів з метою розробити український стандарт криптографічного захисту інформації на заміну ГОСТ 28147-89, в результаті якого було розроблено і розглянуто ряд криптографічних алгоритмів (алгоритм RSB-32, алгоритми «Мухомор», ADE, «Калина», «Лабіринт» та ін.).

Алгоритм асиметричного шифрування вимагає використовувати один ключ для шифрування даних та інший, але взаємопов'язаний з ним ключ — для дешифрування. Один з ключів в такій схемі доступний кожному, хто його запитує. Такий ключ називається відкритим. Інший ключ відомий тільки власникові і називається особистим (закритим або секретним).

Алгоритми асиметричного шифрування виникли у зв'язку з необхідністю передавати секретні ключі по незахищених каналах. Першу систему такого роду розробив Ральф Меркле (Ralph Merkle) в 1974 році. Першим алгоритмом, який завоював широку популярність, був алгоритм Діффі-Хеллмана, створений Уітфілдом Діффі (Whitfield Diffie) і Мартіном Хеллманом (Martin Hellman) в 1976

році. У 1977 році Рон Рівест (Ron Rivest), Аді Шамір (Adi Shamir) і Лен Ейдельман (Len Adleman) розробили схожий алгоритм RSA.

Алгоритм *RSA*

Асиметричний алгоритм RSA відноситься до алгоритмів з відкритим ключем. Першим етапом будь-якого асиметричного алгоритму є створення пари ключів : відкритого й закритого й поширення відкритого ключа по усьому світу.

Криптосистема RSA використовує односторонню функцію утворення добутку двох великих простих цілих чисел (вибираються два прості числа p і q та обчислюється їхній добуток $n = p \times q$), 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

Для ознайомлення з алгоритмом шифрування за схемою RSA, з навчальною метою, слід використати приклад з 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 на відрізку [0,n-1] для деякого n. Для обміну інформацією, зашифрованою за допомогою криптосистеми RSA, необхідно виконати такі кроки.

Крок 1. *Підготовчі обчислення.* Отримувач генерує два (великих) простих числа p і q (мінімум 128-бітних). Для прикладу візьмемо $p = 7$, $q = 11$. 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 $\varphi(77) = 6 \times 10 = 60$. Тепер необхідно згенерувати ціле число, взаємно просте як з n, так і з $\varphi(n)$, наприклад, $e = 13$.

Пара чисел (e,n) буде служити публічним ключем криптосистеми. У нашому випадку це буде пара (13, 77). Тепер необхідно обчислити ***приватний ключ*** d, парний до обра ного 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. 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. Єдиною умовою є захист публічного ключа від підміни. 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 (відкритий) ключ *(e,n)*, у нашому випадку – (13, 77), за допомогою формули $C_i = (M_i)^e \ mod\ n$ 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 українського алфавіту, яка починається з 01) зашифрується таким чином:

$C_1 = 213 \bmod 77 = 30;$
$C_2 = 113 \bmod 77 = 1;$
$C_3 = 1713 \bmod 77 = 73;$
$C_4 = 1413 \bmod 77 = 49.$

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.

Крок 4. *Розшифрування інформації.* Отримувач розшифровує зашифроване повідомлення «30 01 73 49», використавши тільки йому відомий приватний ключ *(d, n)* та формулу $Mi = (Ci)^d \ mod\ n$. 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 зашифрування на публічному та розшифрування на приватному ключі – взаємно зворотні. У цьому випадку приватним ключем служить пара (37,77). Тоді отримаємо: $M_1 = 3037 \bmod 77 = 2$; $M_2 = 1\ 37 \bmod 77 = 1$; $M_3 = 7337 \bmod 77 = = 17$; $M_4 = 4937 \bmod 77 = 14$. Маючи таблицю заміни, за кодами літер отримаємо "БАНК".

Криптосистема RSA симетрична відносно застосування парних ключів: можна зашифровувати інформацію на публічному ключі та розшифровувати на

приватному і навпаки, зашифровувати на приват ному, а розшифровувати – на парному до нього публічному ключі. (Приклади див.літ.)

Алгоритм Ель-Гамаля - криптосистема з відкритим ключем, заснована на труднощі обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Схема Ель-Гамаля лежить в основі стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

Алгоритм (схема) запропонований Тахер Ель-Гамалем в 1985. Ель-Гамаль розробив один із варіантів алгоритму Діффі-Хеллмана. Він удосконалив систему Діффі-Хеллмана і отримав два алгоритми, які використовувалися для шифрування і для забезпечення аутентифікації. На відміну від RSA алгоритм Ель-Гамаля не був запатентований і, тому, став більш дешевою альтернативою, оскільки не вимагалася оплата внесків за ліцензію.

Стійкість криптосистеми Ель-Гамаля ґрунтується на складності задачі дискретного логарифмування у скінченому полі. Для встановлення зашифрованого інформаційного обміну необ хідно виконати наступні 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 $h = g^a\ mod\ n$. 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 наступне:

- 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 формулами: $C_1 = g^r\ mod\ n;$ $C_2 = mh^r\ mod\ n$. Пара чисел C_1 та C_2 утворює шифрограму для числа m.

Крок 3. *Розшифрування інформації.* Розшифрування виконується за формулою: $m = C_2(C_1^a)^{-1}\ mod\ n$. Доведемо це. Підставимо значення C_1 та C_2 у формулу: $m = mh^r (g^a)^{-1}\ mod\ n$. Оскільки $h = g^a\ mod\ n$, то: $m = mh^r (g^a)^{-1}\ mod\ n = mh^r (hr)^{-1}\ mod\ n = m$. Таким чином, доведено еквівалентність прямого та оберненого перетворення.

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.

Швидкість шифрування та розшифрування значно залежить від довжини модуля: збільшення довжини модуля криптосистеми вдвічі призводить до потрійного зростання часу обробки.

ТЕМА 10. СИСТЕМИ ШИФРУВАННЯ ДАНИХ, ЯКІ ПЕРЕДАЮТЬСЯ В МЕРЕЖАХ

10.1. Канальне, наскрізне та комбіноване шифрування.

10.2. Абонементне шифрування.

10.1. Канальне, наскрізне та комбіноване шифрування

Однією з відмінних характеристик будь-якої комп'ютерної мережі є її поділ на так звані рівні, кожен з яких відповідає за дотримання певних умов і виконання функцій, необхідних для спілкування між комп'ютерами, пов'язаними в мережу. Цей поділ на рівні має фундаментальне значення для створення стандартних комп'ютерних мереж. Тому в 1984 р. кілька міжнародних організацій і комітетів об'єднали свої зусилля і виробили приблизну модель комп'ютерної мережі, відому під назвою OSI (Open Systems Interconnection - модель відкритих мережевих з'єднань). Відповідно до моделі OSI комунікаційні функції рознесені по рівнях. Функції кожного рівня незалежні від функцій нижчого вищих рівнів. Кожен рівень може безпосередньо спілкуватися тільки з двома сусідніми.

Модель OSI визначає 7 рівнів: верхні 3 служать для зв'язку з кінцевим користувачем, а нижні 4 орієнтовані на виконання комунікаційних функцій у реальному масштабі часу. Теоретично шифрування даних для передачі по каналах зв'язку комп'ютерної мережі може здійснюватися на будь-якому рівні моделі OSI. На практиці це зазвичай робиться або на самих нижніх, або на самих верхніх рівнях. Якщо дані шифруються на нижніх рівнях, то шифрування називається *канальним*, а якщо на верхніх, то таке шифрування називається *наскрізним*. Обидва ці підходи до шифрування даних мають свої переваги і недоліки.

Канальне шифрування

При канальному шифруванні шифруються абсолютно всі дані, що проходять по кожному каналу зв'язку, включаючи відкритий текст повідомлення, а також інформацію про його маршрутизації і про використовуваний комунікаційний протокол. Однак у цьому випадку будь-який інтелектуальний мережевий вузол (наприклад, комутатор) буде змушений розшифровувати вхідний потік даних, щоб відповідним чином його обробити, знову зашифрувати і передати на інший вузол мережі. Проте канальне шифрування являє собою дуже ефективний засіб захисту інформації в комп'ютерних мережах. Оскільки шифруванню підлягають всі дані, передані від одного вузла мережі до іншого. У криптоаналітика немає ніякої додаткової інформації про те, хто служить джерелом цих даних, кому вони призначені, яка їхня структура і т. д. Але якщо ще подбати і про те, щоб , поки канал простоює, передавати по ньому випадкову бітову послідовність, сторонній спостерігач не зможе навіть сказати, де починається і де закінчується текст переданого повідомлення. Не надто складною є тут робота з ключами. Однаковими ключами слід забезпечити тільки два сусідніх вузла мережі зв'язку, які потім можуть змінювати використовувані ключі незалежно від інших пар вузлів. Найбільший недолік канального шифрування полягає в тому, що дані доводиться шифрувати при передачі по кожному фізичному каналу комп'ютерної мережі. Відправлення інформації в незашифрованому вигляді по якомусь з каналів ставить під загрозу забезпечення безпеки всієї мережі. В результаті вартість реалізації канального шифрування у

великих мережах може виявитися надмірно високою. Крім того, при використанні канального шифрування додатково буде потрібно захищати кожен вузол комп'ютерної мережі, по якому передаються дані. Якщо абоненти мережі повністю довіряють один одному і кожен її вузол розміщений там, де він захищений від зловмисників, на цей недолік канального шифрування можна не звертати уваги. Однак на практиці такий стан зустрічається надзвичайно рідко. Адже в кожній фірмі є конфіденційні дані, знайомитися з якими можуть тільки співробітникиодного певного відділу, а за його межами доступ до цих даних необхідно обмежувати до мінімуму.

Наскрізне шифрування

При наскрізному шифруванні криптографічний алгоритм реалізується на одному з верхніх рівнів моделі OSI. Шифруванню підлягає тільки змістовна частина повідомлення, яке потрібно передати по мережі. Після зашифрування до неї додається службова інформація, необхідна для маршрутизації повідомлення і результат переправляється на більш низькі рівні з метою відправки адресату. Тепер повідомлення не потрібно постійно розшифровувати і зашифровувати при проходженні через кожен проміжний вузол мережі зв'язку. Повідомлення залишається зашифрованим на всьому шляху від відправника до одержувача. Основна проблема, з якою стикаються користувачі мереж, де застосовується наскрізне шифрування, пов'язана з тим, що службова інформація. використовувана для маршрутизації повідомлень, передається по мережі в незашифрованому вигляді. Досвідчений криптоаналітика може отримати для себе масу корисної інформації, знаючи хто з ким, як довго і в які години спілкується через комп'ютерну мережу. Для цього йому навіть не потрібно бути в курсі предмета спілкування. У порівнянні з канальним, наскрізне шифрування характеризується більш складною роботою з ключами, оскільки кожна пара користувачів комп'ютерної мережі повинна бути забезпечена однаковими ключами, перш ніж вони зможуть зв'язатися один з одним. А оскільки криптографічний алгоритм реалізується на верхніх рівнях моделі OSI, доводиться також стикатися з багатьма суттєвими відмінностями в комунікаційних протоколах і інтерфейсах в залежності від типів мереж і об'єднуються в мережу комп'ютерів. Все це ускладнює практичне застосування наскрізного шифрування.

Комбіноване шифрування

Комбінація канального і наскрізного шифрування даних в комп'ютерній мережі обходиться значно дорожче, ніж кожна з них окремо. Однак саме такий підхід дозволяє найкращим чином захистити дані, передані по мережі. Шифрування в кожному каналі зв'язку не дозволяє супротивникові аналізувати службову інформацію, використовувану для маршрутизації. А наскрізне шифрування зменшує ймовірність доступу до незашифрованому даними у вузлах мережі. При комбінованому шифруванні робота з ключами ведеться наступним чином: мережеві адміністратори відповідають за ключі, що використовуються при канальному шифруванні, а про ключі, що застосовуються при наскрізному шифруванні, дбають самі користувачі.

10.2. Абонементне шифрування

ТЕМА 11. ЗАСОБИ УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ

11.1. Генерація ключів.
12.2. Зберігання і розподілення ключів.

ТЕМА 12. ЗАСОБИ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ

12.1. Захист інформації на мережевому рівні.
12.2. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.

12.1. Захист інформації на мережевому рівні

В комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

- міжмережеві екрани (англ. Firewall) - для блокування атак з зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks). Вони керують проходженням мережевого трафіку відповідно до правил (англ. policies) захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і поділяють на внутрішні (приватні) та зовнішні (загального доступу) мережі;
- системи виявлення втручаннь (англ. Intrusion Detection System) - для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (англ. Virtual Private Network) - для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;
- засоби аналізу захищеності - для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

12.2. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність

Протокол мережевої безпеки IPSec

Internet Protocol Security (IPSec) – це узгоджений набір відкритих стандартів, що має на сьогоднішній день конкретну специфікацію, який, в той же час, може бути доповнений 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 забезпе чувати 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 забез-печувати передачу даних у формі, що запобігає їх несанкціонованому перегляду.

Специфікація IP Security (відома сьогодні як IPSec) розробляється робочою групою IP Security Protocol IETF. Спочатку IPsec включав 3 алгоритмо-незалежні базові специфікації, опубліковані в якості RFC- документів «Архітектура безпеки IP», «Автентифікований заголовок (AH)», «Інкапсуляція зашифрованих даних (ESP)» (RFC1825, 1826 і 1827).

У листопаді 1998 року робоча група IP Security Protocol запропонувала нові версії цих специфікацій, що мають в 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 Інтернет 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 Heade» (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 «Інтернет 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 Інтернет Key Exchange» (IKE), є подальшим розвитком і адаптацією ISAKMP, призначений для роботи з протоколами IPSec.

Ядро IPSec складають три протоколи (рисунок 12.1): протокол автентичності (Authentication Header, AH), протокол шифрування (Encapsulation Security Payload, ESP) і протокол обміну ключами (Internet Key Exchange, IKE).

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 конфі-денційність, 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 і ESP частково перекриваються. Протокол AH відповідає тільки за контроль цілісності і автентифікації даних, в той час, як протокол ESP дозволяє шифрувати дані, та виконувати функції протоколу AH (в обмеженому вигляді). Для забезпечення цілісності та автентифікації пакетів даних використовуються спеціальні механізми контролю цілісності та автентичності, які ґрунтуються на присвоєнні даним, що передаються, спеціально сформованої надмірності (коди контролю цілісності та автентичності).

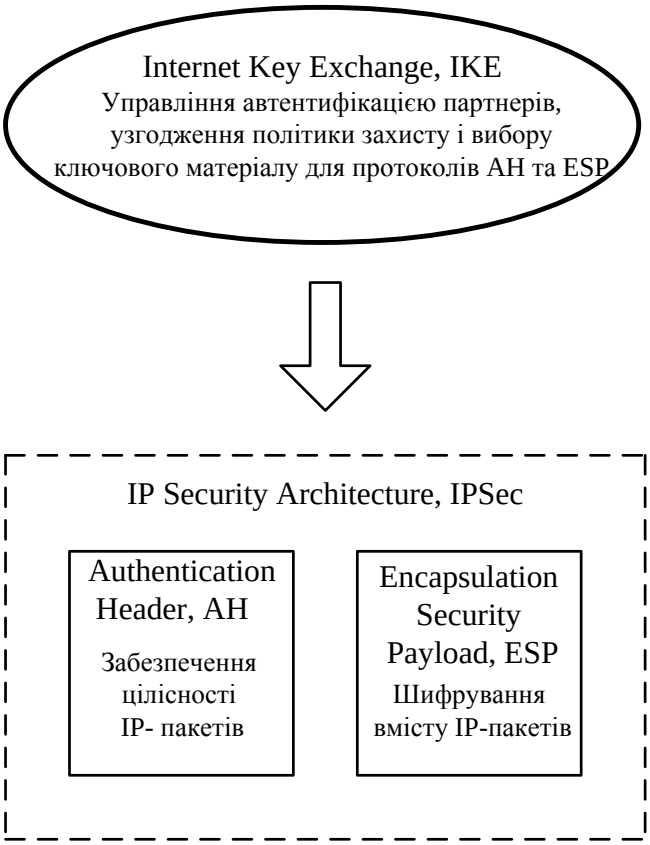

Рисунок 12.1 - Основні компоненти протоколу мережевої безпеки IPSec

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 з взаємної автентифікації сторін. Обрані далі параметри SA визначають, який з двох протоколів, AH чи 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.

У транспортному режимі (рис. 12.) передача IP-пакету виконується за допомогою оригінального заголовка цього пакету 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 АН і ESP притаманні такі недоліки: протокол ESP в транспортному режимі не захищає заголовок пакету даних; неможливо приховати топологію мережі, оскільки заголовки пакетів даних передаються у відкритому (не захищеному) вигляді.

У тунельному режимі (рис. 12.) вихідний IP-пакет поміщається в новий, після чого здійснюється передача даних мережою на підставі заголовка нового IP-пакету.

Цей режим забезпечує захист заголовка пакету даних, у результаті чого ховається топологія мережі, що є безумовною перевагою при побудові 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, що висуваються до захисту даних, а також від ролі, яку відіграє в мережі вузол, завершальний захищений канал. Такий вузол може бути хостом (кінцевим вузлом) або шлюзом (проміжним вузлом).

Протокол ESP може використовуватися як в тунельному, так і в транспортному режимі, самостійно і в комбінації з протоколом АН.

Транспортний режим використовується для захисту поля даних IP пакета, що містить протоколи транспортного рівня (TCP, UDP, ICMP), яке, в свою чергу, містить інформацію прикладних служб.

Прикладом застосування транспортного режиму є передача електронної пошти. Всі проміжні вузли на маршруті пакету від відправника до одержувача використовують тільки відкриту інформацію мережевого рівня і, можливо, деякі опціональні заголовки пакету (в IPv6). Недоліком транспортного режиму є відсутність механізмів приховання конкретних відправника і одержувача пакету, 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 передбачає захист (у тому числі шифрування) всього пакету, включаючи заголовок мережевого рівня. Тунельний режим застосовується у разі потреби приховання інформаційного обміну організації із зовнішнім світом. При цьому, адресні поля заголовка мережевого рівня пакету, що використовує тунельний режим, заповнюються міжмережевим екраном організації і не містять інформації про конкретного відправника пакету. При передачі інформації із зовнішнього світу в локальну мережу організації як адреси призначення використовується мережева адреса міжмережевого екрану. Після розшифрування міжмережевим екраном початкового заголовка мережевого рівня пакет направляється одержувачу.

Протокол SSL

Протокол SSL (secure socket layer) розроблений для забезпечення надійного захисту наскрізної передачі даних з використанням протоколу TCP. SSL становить не один протокол, а два рівні протоколи, як показано на рисунку 12.2.

Протокол SSL пропонує базовий набір засобів захисту, який засто-

совується 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 – служить для автентифікації користувача.

<table>
<tr><td>Протокол квантування SSL</td><td>Протокол зміни параметрів шифрування SSL</td><td>Протокол сповіщення SSL</td><td>HTTP</td></tr>
<tr><td colspan="4">Протокол запису SSL</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

Рисунок 12.2 - Протоколи SSL

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.

ТЕМА 13. АЛГОРИТМИ З ВІДКРИТИМ КЛЮЧЕМ

13.1. Системи захисту PGP та CS MIME.
13.2. Криптографічні функції.
13.3. Сумісність на рівні електронної пошти. Захищена електронна пошта.

ТЕМА 14. ЦИФРОВІ ПІДПИСИ

14.1. Поняття електронного цифрового підпису.
14.2. Стандарти електронних цифрових підписів.
14.3. Основні алгоритми електронного цифрового підпису і їх класифікація.

14.1. Поняття електронного цифрового підпису

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні і некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках.

Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту.

Одним з поширених в світі засобів такого захисту є *електронний цифровий підпис* (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Електронний цифровий підпис (ЕЦП) призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Електронний цифровий підпис використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі. Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Основними визначеннями є :

- *електронний підпис* – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

- *електронний цифровий підпис* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувала; електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

- *засіб електронного цифрового підпису* – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

- *особистий ключ* – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

- *відкритий ключ* – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

- *засвідчення чинності відкритого ключа* – процедура формування сертифіката відкритого ключа;

- *сертифікат відкритого ключа* (далі – сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу; сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

- *посилений сертифікат відкритого ключа* (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

- *акредитація* – процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

- *компрометація особистого ключа* – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

- *підписувач* – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документу.

Програма електронного документообігу з використанням ЕЦП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Звичайний і електронний цифровий підпис

Електронний цифровий підпис може використовуватися юридичними і фізичними особами як аналог власноручного підпису для надання електронному документу юридичної сили. Юридична сила електронного документу, підписаного ЕЦП, еквівалентна юридичній силі документу на паперовому носії, підписаного власноручним підписом особи і скріпленим печаткою.

Електронний цифровий підпис функціонально аналогічний звичайному рукописному підпису на папері.

Закони України прирівнюють за юридичною силою електронні документи, підписані ЕЦП, до документів з власноручним підписом або печаткою, а також створюють правову основу для застосування ЕЦП і здійснення юридично значущих дій шляхом електронного документообігу.

Безпека використання ЕЦП забезпечується тим, що засоби, які використовуються для роботи з ЕЦП, проходять експертизу та сертифікацію в Департаменті спеціальних телекомунікаційних систем СБУ, що гарантує неможливість злому і підробки ЕЦП.

Одним із основних реквізитів документів, що підписуються юридичними особами або фізичними особами-підприємцями, є печатка. Електронний цифровий підпис може також функціонувати і в цій якості. Порядок отримання електронної цифрової печатки юридичними особами і фізичними особами-підприємцями аналогічний порядку отримання електронного цифрового підпису.

Вимоги до цифрового підпису

Аутентифікація захищає двох учасників, які обмінюються повідомленнями, від впливу деякої третьої сторони. Однак проста аутентифікація не захищає учасників один від одного, тоді як і між ними теж можуть виникати певні форми суперечок.

У ситуації, коли обидві сторони не довіряють один одному, необхідно щось більше, ніж аутентифікація на основі загального секрету. Можливим рішенням подібної проблеми є використання цифрового підпису. Цифровий підпис повинний володіти наступними властивостями:

1. Повинна бути можливість перевірити автора, дату і час створення підпису.

2. Повинна бути можливість аутентифікувати вміст під час створення підпису.

3. Підпис повинен бути перевірений третьою стороною для вирішення спорів.

Таким чином, функція цифрового підпису включає функцію аутентифікації. На підставі цих властивостей можна сформулювати наступні вимоги до цифрового підпису:

1. Підпис повинен бути двійкового зразком, який залежить від підписується повідомлення.

2. Підпис повинен використовувати деяку унікальну інформацію відправника для запобігання підробки або відмови.

3. Створювати цифровий підпис повинно бути відносно легко.

4. Повинно бути обчислювально неможливо підробити цифровий підпис як створенням нового повідомлення для існуючої цифрового підпису, так і створенням помилкової цифрового підпису для деякого повідомлення.

5. Цифровий підпис має бути досить компактним і не займати багато пам'яті.

Існує кілька підходів до використання функції цифрового підпису. Всі вони можуть бути розділені на дві категорії: *прямі та арбітражні*.

При використанні прямого цифрового підпису взаємодіють тільки самі учасники, тобто відправник та одержувач. Передбачається, що одержувач знає відкритий ключ відправника. Цифровий підпис може бути створений шифруванням усього повідомлення або його хеш-коду (перетворення вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини) закритим ключем відправника.

Конфіденційність може бути забезпечена подальшим шифруванням усього повідомлення разом з підписом відкритим ключем одержувача (асиметричне шифрування) або розділяються секретним ключем (симетричне шифрування). Зазвичай функція підпису виконується першою, і тільки після цього виконується функція конфіденційності. У разі виникнення спору якась третя сторона повинна переглянути повідомлення і його підпис. Якщо функція підпису виконується над зашифрованим повідомленням, то для вирішення спорів доведеться зберігати повідомлення як в незашифрованому вигляді (для практичного використання), так і в зашифрованому (для перевірки підпису). Або в цьому випадку необхідно зберігати ключ симетричного шифрування, для того щоб можна було перевірити підпис початкового повідомлення. Якщо цифровий підпис виконується над незашифрованим повідомленням, одержувач може зберігати тільки повідомлення в незашифрованому вигляді і відповідний підпис до нього.

Всі прямі схеми мають спільне слабке місце. Дієвість схеми залежить від безпеки закритого ключа відправника. Якщо відправник згодом не захоче визнати факт відправлення повідомлення, він може стверджувати, що закритий ключ був втрачений або вкрадений, і в результаті хтось підробив його підпис. Можна застосувати адміністративне управління, що забезпечує безпеку закритих ключів, для того щоб, принаймні, хоч у якійсь мірі послабив ці загрози. Один з можливих

способів полягає у вимозі до кожного підпису повідомлення включати позначку часу (дату і час) і повідомляти про скомпрометовані ключі в спеціальний центр.

Інша загроза полягає в тому, що закритий ключ може бути дійсно вкрадений у X в момент часу T. Порушник може потім послати повідомлення, підписане підписом X і позначений тимчасовою міткою, яка менше або дорівнює T.

Проблеми, пов'язані з прямим цифровим підписом, можуть бути частково вирішені за допомогою *арбітра.* Існують різні схеми з застосуванням арбітражного підпису. У загальному вигляді арбітражний підпис виконується наступним чином. Кожне підписане повідомлення від відправника до одержувача X Y першою справою надходить до арбітра A, який перевіряє підпис для цього повідомлення. Після цього повідомлення датується і надсилається до Y із зазначенням того, що воно було підтверджено арбітром. Присутність A вирішує проблему схем прямого цифрового підпису, при яких X може відмовитися від повідомлення.

14.2. Стандарти електронних цифрових підписів

Цифровий підпис у відповідності зі стандартом ISO 7498-2 представляє собою отримані, в результаті криптографічного перетворення блоку даних, дані, які дозволяють одержувачу упевнитися в цілісності цього блоку та автентичності джерела, а також забезпечує захист від підробки одержувача. Цифровий підпис дозволяє з високим ступенем достовірності визначити джерело повідомлення або даних.

Стандарти цифрового підпису наведено в таблиці 14.1.

Таблиця 14.1 - Стандарти цифрових підписів

№ п/п	Тип цифрового підпису	Стандарт
1	RSA схема	ISO 9796, 11166
2	DSA схема	NIST MD-20899
3	DSA подібна схема	ГОСТ 34.10-94

Усі стандарти припускають несиметричну схему формування і перевірки цифрового підпису. Для виконання цих процедур використовуються різні ключі. Для установлення цифрового підпису - т. н. конфіденційні, а для перевірки цифрового підпису - відкриті ключі. Тому додатково з цими схемами використовуються стандарти для роботи з відкритими ключами, наприклад, стандарт для угоди про ключі Діффі-Хелман (X9.42).

Усі стандарти передбачають використання загальномережевих параметрів. В алгоритмі RSA в якості загальномережевого параметра використовується модуль перетворення

$$N = P * Q,$$

де P, Q прості числа (бажано сильні) необхідної розрядності.

Юридичне забезпечення електронного підпису

Верховною Радою України прийнято Закон України «Про електронний цифровий підпис» від 22.05.2003 N 852-IV (далі - Закон). Відповідно до частини 1 статті 18 Закону він набирає чинності з 1 січня 2004 року.

Цей Закон визначає правовий статус електронного цифрового підпису (ЕЦП) та регулює відносини, що виникають при використанні електронного цифрового підпису.

Згідно зі статтею 1 Закону електронний підпис - *дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;* електронний цифровий підпис - *вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.*

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Закон окреслює коло суб'єктів правових відносин у сфері послуг електронного цифрового підпису, його призначення та особливості застосування.

Необхідно особливо підкреслити, що в реалізації цього Закону найбільш зацікавлені на поточний момент банківська система та податкова система України, торгівля, тощо.

Відповідно до статті 4 Закону електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Відповідно до статті 15 Закону особи, винні у порушенні законодавства про електронний цифровий підпис, несуть відповідальність згідно з законом.

14.3. Основні алгоритми електронного цифрового підпису і їх класифікація

Основними стандартами ЕЦП є:

- міжнародний стандарт ISO/IEC 9796, який визначає ЕЦП з відновленням повідомлення (digital signature with message recovery);
- міжнародний стандарт ISO/ IEC 14888, який визначає ЕЦП з дода ванням (digital signature with appendix);
- російський стандарт цифрового підпису на еліптичній кривій ГОСТ

Р34.10-2001;

- американський національний стандарт цифрового підпису (FIPS 186);
- американський фінансовий стандарт цифрового підпису з додаванням еліптичної кривої (ANSI X9.62);
- стандарт на ЕЦП PKCS #1, який визначає ЕЦП на основі алгоритму RSA; стандарт цифрового підпису з додаванням і відновленням повідомлення IEEE 1363;
- стандарт цифрового підпису з додаванням еліптичної кривої IEEE P1363; міжнародний стандарт ISO/IEC CD 15946-2 стандартизується ЕЦП еліптичною кривою з додаванням;
- Державний стандарт України ДСТУ-4145 – 2002.

На основі існуючих стандартів ЕЦП запропонована класифікація ЕЦП.

За способом побудови схеми ЕЦП діляться на два класи:

- схема ЕЦП із відновленням повідомлення;
- схема ЕЦП із додаванням.

За кількістю учасників ЕЦП підрозділяється на:

- одиночну схему ЕЦП;
- групову схему ЕЦП.

У процесі виконання алгоритму формування цифрового підпису в одиночних схемах ЕЦП досить одного учасника, у групових схемах їх два або більше.

За способом перевірки ЕЦП поділяються на два класи:

- інтерактивні схеми ЕЦП, що вимагають протокольної взаємодії;
- не інтерактивні схеми ЕЦП, які не потребують протокольної взаємодії.

Існуючі алгоритми ЕЦП можна розділити також за типами використовуваних односпрямованих функцій із секретом:

- схеми ЕЦП, засновані на стійкості факторизації великого числа;
- схеми ЕЦП, засновані на стійкості дискретного логарифма;
- схеми ЕЦП, засновані на стійкості дискретного логарифма в групі точок ЕК.

Кожна з цих схем може бути детермінована або рандомована. Застосування детермінованих схем характеризується тим, що цифровий підпис одним і тим же вхідним рядком даних приводить до формування однакових цифрових підписів. У рандомованій схемі при генерації підпису використовується деякий випадковий параметр, що приводить до формування різних підписів, навіть для однакових вхідних рядків. У рандомізованих схемах необхідно забезпечити непередбачуваність випадкових чисел. У свою чергу детерміновані схеми діляться на схеми ЕЦП одноразового застосування і схеми ЕЦП багаторазового застосування.

Цифрові підписи з відновленням повідомлення є об’єктом розгляду двох стандартів ISO/IEC 9796 (1991 року) і ISO/IEC 9796-2 (1997 року). У стадії розробки перебуває четверта частина стандарту ISO/IEC 9796-4. Механізми ЕЦП певні в ISO/IEC 9796 застосовуються тільки до коротких повідомлень, тоді як механізми ISO/IEC 9796-2 застосовуються до повідомлень довільної довжини. Стандарт ISO/IEC 14888 визначає механізми ЕЦП другого класу. Дані механізми

застосовані до повідомлень довільної довжини. При обчисленні цифрових підписів з додаванням особливу роль відіграють однобічні геш-функції. Геш-функції також є об'єктом міжнародної стандартизації. Зокрема основним нормативним документом у даній області є міжнародний стандарт ISO/IEC 10118. Він складається з декількох частин і вводить модель геш-функції (ISO/IEC 10118-1(1994 року), розглядає два методи для побудови геш-функцій на основі блокових шифрів (ISO/IEC 10118-2 (1994 року), визначає три спеціалі- зованих (dedicated) геш-функції, тобто геш-функції, які розроблені спеціально для обчислення контрольних сум (ISO/IEC 10118-3 (1998 року).

Відомі методи забезпечення автентичності та цілісності даних засновані на внесенні надмірності (імітовставки, коду автентифікації, цифрового підпису) в оброблювану послідовність. В останні роки ця галузь знань бурхливо розвивається, запропоновано велику кількість різних криптографічних методів і алгоритмів. Найбільшого поширення набули протоколи, засновані на використанні односторонніх геш-функцій

ТЕМА 15. ПАРОЛІ І МЕХАНІЗМИ КОНТРОЛЮ ЗА ДОСТУПОМ

15.1. Основні принципи захисту інформації при підключенні до мережі Інтернет.

15.2. Моделі управління доступом

15.1. Основні принципи захисту інформації при підключенні до мережі Інтернет

Для підключення будь-якої організації до мережі Інтернет 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 вище 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 Інтернет порівняно простими засобами.

Firewall (Брандмауер)

Основним загальновизнаним засобом такого захисту є міжмережний екран (брандмауер). Міжмережний екран установлюється між мережею та Інтернет і виконує роль мережевого фільтра (рисунок. 15.1).

Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Інтернет і назад, і обмежити трафік з боку Інтернет 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 Інтернет і двонаправлений доступ між Інтернет 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 пара метри 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 допо- могою 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 Інтернет- інтерфейсу, 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.

Крім того, 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. З найбільш дешевих систем слід зазначити Firewall на основі ядра операційної системи Linux версії 2.4.20 і вище й засоби керування iptables. Через те, що Linux є безкоштовною ОС, витрати на побудову такого міжмережного екрана зводяться до придбання звичайного персонального комп'ютера із двома мережними інтерфейсами. Проте Linux дозволяє побудувати досить надійний і гнучкий мережний фільтр, що розпізнає окремі прапори в службових полях IP-пакета.

NAT

Другою складовою забезпечення захищеності мережі є "заміна мережної адреси" – Network Address Translation, або 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 вико ристання діапазонів адрес, які не застосовуються в Інтернет (наприклад, 10.0.0.0 – 10.255.255.255). Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп'ютерів і приховує структуру мережі. Існує кілька різно видів NAT. Найпростіша й найбільш марна з погляду захисту – це 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 потрібно забезпечити доступ ззовні (рисунок 15.2).

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 доступ зловмиснику, тому що повністю приховує внутрішні комп'ютери й перешкоджає "вичисленню" об'єкту вторгнення (рисунок 15.3). 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.

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'єднан- ня може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі противнику, 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. Звичайно це поштовий, dns і web-сервери. Механізм їх роботи допускає, що до них повинен бути дозволений вільний або слабко обмежений доступ з Інтернету. Відповідно ймовірність їх зламу вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, яка захищається, недоцільно з погляду 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* (рисунок 15.4).

Proxy-сервер

Використання так званого «посередника» (proxy-сервера) також підвищує рівень захищеності мережі, тому що виключає необхідність прямого виходу в Інтернет 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 Інтернет. Схематично сутність його роботи показана на рисунку 15.5.

Proxy-сервер складається ніби із двох частин – клієнтської і серверної. Клієнтська частина дивиться у бік Інтернету, серверна – у бік клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до виділеного сайту через proxy-сервер, його клієнтський мережний додаток взаємодіє із серверною частиною proxy-сервера. При цьому proxy-сервер на рівні додатку 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 proxy-сервера.

Після цього, 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 виділеним сайтом виключається. Усередині proxy-сервера передача даних між клієнтською частиною й серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатку, що забезпечується легкість контролю команд і даних на відповідність установленим стандартам. Крім того, це дозволяє забезпечити досить надійний контроль проти передачі зловмисних кодів усередині даних. Навіть у випадку успішної атаки з боку Інтернет за відкритими протоколами у цьому випадку буде ушкоджений тільки proxy-сервер, 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 та інших) і не пропускає через себе інші пакети, він сильно обмежує можливості зловмисників з використання мережних "троянських коней" для закріплення на будь-якому з користувальницьких комп'ютерів.

Антивірусний захист поштової системи

Операційна система Windows дуже вразлива перед деякими різновидами

поштових вірусів. Користувачу буває досить встановити покажчик на інфікований конверт, щоб вірус активізувався. Але більш небезпечним є те, що механізм роботи поштових вірусів може бути використаний зловмисником для закидання в область, яка захищається, мережного "троянського коня". Він дозволить противнику таємно скачувати дані мережі та здобути всю інформацію, що цікавить. Тому забезпеченню антивірусного захисту тракту доставки пошти у внутрішню мережу варто приділити досить 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 вся пошта, що проходить через сервер, спочатку перенаправляється спеціальному користувачу, у ролі якого виступає антивірусний процес. Він сканує зміст кожного аркуша 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 аркушу, а також на ім'я зазначених адміністраторів системи. Після перевірки аркуші, що не викликають підозри, відсилаються за призначенням.

Тим самим на рівні поштового сервера ставиться 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

Розроблювачі програмного забезпечення включають у свої продукти фрагменти коду, які на ту або іншу подію генерують відповідні текстові повідомлення, які посилають 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 корисні log-файли для пошуку слідів зламу системи і відвідування її несанкціонованими гостями. Через те, що злом, як правило, супроводжується множиною заборонених дій, це породжує велику кількість системних повідомлень, що осідають в log-файлах. Із цієї причини зловмисник завжди прагне стерти сліди своєї присутності, або видаливши log-файли, або їх підчистивши. В обох випадках адміністратору після цього буде важко зрозуміти, що ж відбулося в системі насправді – яким чином у неї проникнули, як довго в ній перебували.

Тому обов'язковою умовою для мережі, підключеної до Інтернету, 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 виділений сервер. Це можуть робити також маршрутизатори й міжмережні екрани. Збираючи такі повідомлення на спеціально виділеному сервері, забезпечується можливість їх збереження від втручання зловмисника. Тому для мінімізації ймовірності зламу log-сервер повинен бути призначений

тільки для збору log-повідомлень. Він не повинен виконувати будь-яких інших функцій і виконувати інші мережні додатки, крім syslogd. У цьому випадку після зламу будь-яких комп’ютерів мережі на log- сервері залишаться відповідні повідомлення, знищити які зловмисник уже не зможе. Таким чином, у результаті найбільш оптимальною є наступна схема підключення локальної мережі до Інтернет (рис. 15.6).

Таким чином, проведений аналіз способів захисту комп’ютерних мереж при підключені їх до глобальної мережі Інтернет показав, що для забезпечення захисту при обміні інформацією абоненти локальної мережі повинні використовувати принципи і засоби безпеки в комплексі з організаційними заходами.

15.2. Моделі управління доступом

Моделі управління доступом визначають правила управління доступом до інформації, дозволами в системі так, щоб система завжди була безпечною.

Властивості моделей управління доступом:

1) Модель управління доступом повинна бути адекватною модельованій системі.

2) Модель повинна бути простою і абстрактною і не складною для розуміння.

Існують матричні та багаторівневі моделі управління доступом.

Матричні моделі управління доступом:

Модель Лемпсона

Дана модель дозволяє динамічно передавати права об'єктів. Основа моделі - правила доступу, що визначають можливий вид доступу суб'єкта до об'єкта доступу. Як об'єкти виступають пасивні елементи матриці. Як суб'єкти – активні елементи. Суб'єкти можуть бути також і об'єктами доступу.

Недоліки цієї моделі:

- не всі суб'єкти доступу мають доступ до всіх об'єктів (матриця сильно розріджена);
- дана модель не відстежує потоки інформації.

Модифікації моделі Лемпсона:

1) *Списки управління доступом до об'єктів.* У даній моделі повноваження доступу визначаються у вигляді списку кортежів для всіх суб'єктів, що мають доступ до даного об'єкту. Така модель застосовується в системах Novell.

Переваги даної моделі:

- економія пам'яті;
- зручність отримання відомостей про суб'єктів, що мають доступ до даного об'єкту.

Недоліки:

- незручність отримання відомостей про об'єкти, до яких має доступ даний суб'єкт;
- незручність відстежування обмежень і залежностей.

2) *Списки повноважень суб'єктів (профіль суб'єкта).* У даній моделі повноваження доступу суб'єкта представляються у вигляді списку кортежів для всіх об'єктів, до яких він має доступ. Профіль суб'єкта використовується для відстежування подій аудиту в ОС Microsoft Windows NT.

Переваги моделі:

- економія пам'яті;
- зручність отримання відомостей про об'єкти, до яких має доступ даний суб'єкт.

Недолік: незручність отримання відомостей про суб'єктів, які мають доступ до даного об'єкта.

Атрибутна схема

Атрибутні способи задання матриці доступу засновані на привласненні суб'єктам і об'єктам певних міток (атрибутів, що містять значення). Така схема використовується в ОС сімейства UNIX. Матриця задана в неявному вигляді. Обчислення рівня доступу суб'єкта до об'єкта відбувається динамічно.

При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним з них залишається парольний захист. Для цього є декілька причин з яких слід відзначити наступні:

- *відносна простота реалізації*. Дійсно, реалізація механізму парольного захисту зазвичай не вимагає залучення додаткових апаратних засобів.
- *традиційність*. Механізми парольного захисту є звичними для більшості користувачів автоматизованих систем і не викликають психологічного несприйняття – на відмінну, наприклад, від сканерів малюнка сітківки ока.

Для парольних систем захисту характерний парадокс, що ускладнює їх ефективну реалізацію: стійкі паролі мало придатні для використання людиною. Дійсно, стійкість пароля прямо пропорційна його складності. Однак чим складніший пароль, тим важче його запам'ятати, і у користувача з'являється спокуса записати незручний пароль, що створює додаткові канали для його дискредитації.

В загальному випадку пароль може бути отриманий зловмисником одним з трьох поширених способів:

1) *За рахунок використання людського фактору.* Методи отримання паролів тут можуть бути самими різними:

a) підглядання.
b) підслуховування.
c) шантаж.
d) загрози
e) зрештою, використання чужих облікових записів з дозволу їх законних власників.

2) *Шляхом підбору.* При цьому використовуються наступні методи:

- п*овний перебір*. Даний метод дозволяє підібрати будь-який пароль незалежно від його складності. Проте час, необхідний для реалізації даної атаки, для стійкого пароля буде досить значним і логічно припустити, що він буде суттєво перевищувати допустимі ресурси часу, наявного у зловмисника;

- п*ідбір по словнику*. Значна частина паролів, що використовуються на практиці є осмисленими словами або виразами. Існують словники найпоширеніших паролів, які у багатьох випадках дозволяють обійтися без повного перебору.

3) *Підбір з використанням відомостей про користувача.* Даний інтелектуальний метод підбору паролів грунтується на тому факті, що якщо політика безпеки системи передбачає самостійне призначення паролів користувачами, то в переважній більшості випадків у якості паролю буде обрана якась персональна інформація, пов'язана з користувачем КС. І хоча такою інформацією може бути вибрано що завгодно, від дати народження коханої людини і до прізвиська улюбленого песика, наявність певної інформації про користувача дозволяє перевірити найбільш поширені варіанти (дні народження, імена дітей і т.д.).

4) За рахунок використання недоліків реалізації парольних систем. До таких недоліків реалізації відносяться експлуатовані уразливості мережевих сервісів, що реалізовують певні компоненти парольної системи захисту або ж недекларовані можливості відповідного програмного або апаратного забезпечення.

При побудові системи парольного захисту необхідно враховувати специфіку КС і керуватися результатами проведеного аналізу ризиків. В той же час можна привести наступні практичні рекомендації:

- в***становлення мінімальної довжини пароля***. Очевидно, що регламентація мінімально допустимої довжини пароля суттєво ускладнює для зловмисника реалізацію підбору пароля шляхом повного перебору;

- ***збільшення потужності алфавіту паролів***. За рахунок збільшення потужності (яке досягається, наприклад, шляхом обов'язкового використання спецсимволів) також можна ускладнити повний перебір;

- ***перевірка і вібраковування паролів за словником***. Даний механізм дозволяє ускладнити підбір паролів за словником за рахунок ***відбраковування*** явно «підбирабельних» паролів;

- ***встановлення максимального терміну дії пароля.*** Термін дії пароля обмежує проміжок часу, який зловмисник може затрачувати на підбір пароля. Тим самим, скорочення терміну дії пароля зменшує вірогідність його успішного підбору:

- ***віббраковування по журналу історії паролів.*** Механізм запобігає повторному використання паролів – можливо, раніше скомпрометованих;

- ***обмеження числа спроб введення пароля.*** Відповідний механізм ускладнює інтерактивний підбір паролів;

- ***примусова зміна пароля при першому вході користувача в систему.*** У випадку якщо первинну генерацію паролів для всіх користувач здійснює адміністратор, користувачу може бути запропоновано змінити первинний пароль при першому ж вході в систему – в цьому випадку новий пароль не буде відомий адміністратору;

- ***затримка при введенні неправильного пароля.*** Механізм перешкоджає інтерактивному підбору паролів;

- ***заборона вибору пароля користувачем і автоматична генерація пароля.*** Даний механізм дозволяє гарантувати стійкість згенерованих паролів, проте варто усвідомлювати, що в цьому випадку у користувачів можуть виникнути проблеми із запам'ятовуванням паролів.