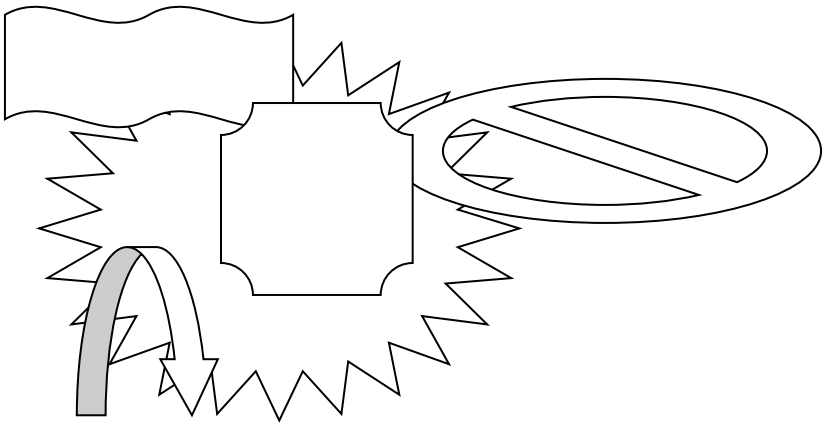
Міністерство освіти і науки України
Національний педагогічний університет
імені М. П. Драгоманова

С. М. Яшанов, М. С. Яшанов

Безпека інформаційних технологій

Навчально-методичний посібник



Київ
Вид-во НПУ імені М. П. Драгоманова
2019

УДК 378.091.33-027.22:004(076)
Я 96

Друкується за ухвалою Вченої ради
Національного педагогічного університету імені М. П. Драгоманова
(протокол № 12 від 05 квітня 2018 р.)

Рецензенти: *М. І. Жалдак*, академік АПН України, доктор педагогічних наук, професор, завідувач кафедри теоретичної інформатики НПУ імені М. П. Драгоманова;
Л. Д. Шевчук, кандидат педагогічних наук, доцент, завідувач кафедри математики, інформатики та методики навчання Державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди».

Яшанов С. М.

Я 96 Безпека інформаційних технологій : навчально-методичний посібник / С. М. Яшанов, М. С. Яшанов. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2019. – 255 с.

У навчально-методичному посібнику розглядаються методи і засоби забезпечення інформаційної безпеки та компоненти систем захисту комп'ютерних систем і технологій. Описуються засоби реалізації механізмів безпеки в комп'ютерних системах і технологіях. Окрему увагу приділено інформаційній безпеці та організаційно-правовому захисту інформації.

Для студентів напрямку «Професійна освіта. Комп'ютерні технології» денної та заочної форм навчання.

УДК 378.091.33-027.22:004(076)

Зміст

Розділ ІІ

РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ І ТЕХНОЛОГІЯХ

Вступ

Новий етап у розвитку обміну інформацією, що характеризується інтенсивним впровадженням сучасних комп'ютерних технологій, широким поширенням локальних, корпоративних і глобальних мереж у всіх сферах життя інформаційного суспільства, створює нові можливості та якість інформаційного обміну. У зв'язку з цим проблеми інформаційної безпеки (ІБ) набувають першорядного значення, актуальність та важливість яких обумовлена такими факторами:

• високі темпи зростання парку комп'ютерних засобів, що застосовуються у різних сферах діяльності, і, як наслідок, різке розширення кола користувачів, які мають безпосередній доступ до обчислювальних мереж та інформаційних ресурсів;

• збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою ПК та інших засобів автоматизації;

• бурхливий розвиток апаратно-програмних засобів та технологій, що не відповідають сучасним вимогам безпеки;

• невідповідність бурхливого розвитку засобів обробки інформації та опрацювання теорії ІБ розробки міжнародних стандартів та правових норм, що забезпечують необхідний рівень захисту інформації (ЗІ);

• повсюдне поширення мережевих технологій, створення єдиного інформаційно-комунікаційного світового простору на базі мережі Інтернет, яка за своєю ідеологією не забезпечує достатнього рівня ІБ.

Зазначені вище чинники створюють певний спектр загроз ІБ лише на рівні особистості, нашого суспільства та держави. Засобом нейтралізації значної частини є формування теорії ІБ і методології захисту інформації.

Отже, у цьому сенсі, безпека інформаційних систем і технологій багато в чому залежить від якісного ведення поточної роботи, яка включає: підтримку користувачів і програмного забезпечення; конфігураційне управління і резервне копіювання; управління носіями і документування; регламентні роботи тощо.

Сучасні комп'ютерні системи (КС), інформаційні системи та інформаційні технології (ІС та ІТ) складні і, отже, вразливі вже самі по собі, навіть без урахування активності зловмисників. Постійно виявляються нові вузькі місця в їх інформаційно-технологічному забезпеченні, тому при організації інформаційної безпеки доводиться брати до уваги надзвичайно широкий спектр апаратного і програмного забезпечення та численні зв'язки між компонентами цих систем.

Це пов'язано з тим, що на сьогодні надзвичайно швидко змінюються принципи побудови корпоративних ІС, використовуються численні зовнішні інформаційні сервіси та надаються назовні власні. Надзвичайно швидко набув поширення аутсорсінг, коли частина функцій корпоративної ІС передається зовнішнім організаціям, розвивається програмування з активними агентами.

Ще одним підтвердженням складності проблематики безпеки інформаційних технологій в комп'ютерних системах є паралельне (і досить швидке) зростання витрат на захисні заходи і зростання кількості порушень інформаційної безпеки у поєднанні зі збільшенням збитків від кожного порушення.

Зміст навчально-методичного посібника спрямований на формування інформатичної компетентності фахівців освітньої галузі на основі системи теоретичних і методологічних знань, спеціальних умінь у галузі інформаційної безпеки та захисту інформації та їх використання у професійній діяльності.

Розділ 1

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І ТЕХНОЛОГІЙ

Тема 1. Загальні підходи до забезпечення інформаційної безпеки в комп'ютерних системах і технологіях

Розвиток комп'ютерних засобів передавання, приймання, оброблення інформації та поширення вимагають розробки методів технічних та програмних засобів забезпечення захищеності інформації. Слід також відзначити і необхідність вжиття заходів щодо забезпечення інформаційної безпеки суспільства. Масштаби і сфери застосування комп'ютерної техніки і технології стали такі, що поряд з надійністю її функціонування постає питання не тільки захисту інформації, а й інформаційної безпеки її власника і споживача, кому вона призначається. Вирішення цієї проблеми, незважаючи на великий обсяг проведених досліджень, класифікації об'єктів обробки інформації, методів визначення можливих каналів несанкціонованого доступу (НСД), методів розрахунку міцності захисту інформації, ускладнюється відсутністю єдиної теорії і концепції забезпечення інформаційної безпеки в комп'ютерних системах і технологіях.

З появою складних інформаційних систем управління, пов'язаних з автоматизованим зберіганням, обробленням і виведенням інформації, проблема її захисту обумовлена:

- збільшенням обсягів інформації, що накопичується, зберігається та обробляється за допомогою ЕОМ та інших засобів комп'ютерної техніки;
- зосередженням в єдиних базах даних інформації різного призначення і приналежності;
- розширенням кола користувачів, що мають доступ до ресурсів інформаційних систем і масивів даних, що знаходяться в ній;
- ускладненням режимів функціонування технічних засобів комп'ютерної техніки та широке впровадження багатопрограмного режиму, режиму розподілу часу і реального часу;
- автоматизацією міжмашинного обміну інформацією, в тому числі і на великих відстанях;
- збільшенням кількості технічних засобів зв'язку в автоматизованих системах управління і оброблення даних;
- появою персональних комп'ютерів, що розширюють можливості не тільки користувачам, але і зловмисників.

Розвиток інформаційних технологій призвів до появи нового виду злочину – спеціальні комп'ютерні зловмисники: хакери, крекери. Хакери (Hacker, анг.) – комп'ютерний хуліган, який одержує задоволення від проникнення в чужий комп'ютер. Крекерів (cracker, англ.) – злодій-зломщик.

Наслідки несанкціонованих впливів і несанкціонованого використання інформації завдають величезної шкоди політичного, економічного характеру, що ставить на грань життя земної цивілізації. Є великий перелік прикладів несанкціонованого запуску бойових машин.

Для запобігання можливим інцидентам проводиться робота із вдосконалення правових і юридичних норм в галузі комп'ютерної технології. При розробці заходів щодо забезпечення інформаційної безпеки слід дотримуватись таких вимог:

- вибір інформації в якості предмета захисту (ресурси теж захищаються, але тільки в необхідних випадках);
- використання в розрахунках міцності захисту часу життя інформації;
- використання в побудові захисту класифікацію інформаційних систем за видами, принципам побудови та оброблення даних;
- застосування різних підходів до ненавмисних і навмисних загроз інформації;
- долучення відомої стратегії і тактики захисту будь-якого об'єкта до інформаційної безпеки в комп'ютерних системах і технологіях;
- зведення всіх потенційних загроз до трьох подій: витоку, модифікації і втрати;
- розробка і використання в постановці завдання простої моделі очікуваного поведінки порушника і його класифікації;
- визначення в інформаційних системах і технологіях можливих каналів несанкціонованого доступу до інформації з боку порушника того чи іншого класу;
- розробці розрахункових співвідношень для побудови засобів і систем захисту, що перекривають можливі канали несанкціонованого доступу.

При розробці засобів інформаційної безпеки розробник повинен керуватися наступним:

- створенням основ єдиної, для всіх видів інформаційних систем, теорії безпеки інформації;
- створенням, в заданій інформаційній системі, вбудованої автоматизованої підсистему безпеки інформації у вигляді єдиного механізму з гарантованими кількісними і якісними характеристиками;
- досягненням можливості отримання з позицій безпеки інформації оптимальних вимог до апаратних і програмних засобів ІС;
- досягненням можливості включення типових вимог з безпеки інформації в технічне завдання на розробку комп'ютерної системи;

• необхідністю розробки чітких і ясних керівних нормативних документів з безпеки інформації при створенні комп'ютерних систем.

Таким чином, захист інформації, а також інформаційні відносини вимагають ретельного опрацювання кримінально-правового захисту, тому що інформація і інформаційні відносини в цьому випадку є об'єктом злочину.

1.1. Правові та нормативні акти, що кваліфікують інформаційні комп'ютерні злочини

Опрацювання правової основи, законодавства і положення щодо їх застосування необхідна для успішної роботи із забезпечення достатнього рівня інформаційної безпеки. Це продиктовано особливостями, притаманними для інформаційних злочинів з використанням високих комп'ютерних технологій, а також проблемами інформаційних нападів і злочинів.

Проблема інформаційних нападів. Як показує аналіз, зростання злочинності в галузі інформаційних технологій є практично неконтрольованим процесом. Практично всі державні і комерційні структури піддаються інформаційному нападу, наслідки яких не афішуються. Це ускладнює можливості проводити цілеспрямовану профілактичну роботу щодо запобігання подібного виду злочину. Факти говорять про збитки тільки американських компаній, які обчислюються сотнями мільярдів доларів. На українському ринку програмного забезпечення щомісячно фіксується поява більш 10 нових вірусів. Зареєстровані факти розкрадань з українських банків на мільйони доларів і разові спроби розкрадань, що перевищують 50 млрд гривень. Все частіше фіксуються спроби проникнення в інформаційні мережі банківських організацій України. Понад 50% з тих, хто випробував вторгнення або проводив дослідження, встановив факт несанкціонованих дій з боку своїх співробітників. Опитування

власників і законних користувачів інформаційних мереж показав, що понад 50% не мають плану заходів на випадок несанкціонованого вторгнення. Понад 60% не мають стратегії збереження докази порушень для подальшого судового та кримінального розгляду. Понад 70% розглядають можливість звернення до правоохоронних органів як «антирекламу».

Всі ці передумови змушують необхідність з'ясування основних понять – «інформація», «інформаційний процес», «комп'ютер» для правового регулювання і сукупності поняття нормативного регулювання в Україні інформаційних відносин і визначити стан правового забезпечення ситуації, чинною в даній галузі.

Проблема інформаційних злочинів. Розвиток термінологічного апарату дозволяє сформулювати нові термінологічні визначення видів інформаційних злочинів. Слід зазначити такі найменування як «комп'ютерні злочини», «комунікаційні злочину», «кібербандитизм». При проведенні розслідувань інформаційних несанкціонованих дій термінологічна неточність тлумачення закону або методологічних рекомендацій з його виконання може спричинити неправильне його застосування. Тому необхідно знати правові законодавчі визначення та термінологію, що регулюють правила розслідувань ситуацій, які потягли за собою кримінальну відповідальність.

Відповідно до чинного законодавства: **інформаційні правовідносини** – це відносини, що виникають при: формуванні та використанні інформаційних ресурсів на основі створення, збирання, оброблення, накопичення, зберігання, пошуку, розповсюдження і надання споживачеві документованої інформації; створенні та використанні інформаційних технологій і засобів їх забезпечення; захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації.

На основі чинного законодавства прийняті в такому значенні:

1. Інформація – відомості про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання.

2. Інформатизація – організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для задоволення інформаційних потреб і реалізації прав громадян, органів державної влади, органів місцевого самоврядування, організацій, громадських об'єднань на основі формування і використання інформаційних ресурсів.

3. Документована інформація (документ) – зафіксована на матеріальному носії інформація з реквізитами, що дозволяють її ідентифікувати.

4. Інформаційні процеси – процеси збирання, оброблення, накопичення, зберігання, пошуку і розповсюдження інформації.

5. Інформаційна система – організаційно впорядкована сукупність документів (масивів документів) та інформаційних технологій, у тому числі з використанням засобів обчислювальної техніки і зв'язку, що реалізують інформаційні процеси.

6. Інформаційні ресурси – окремі документи і окремі масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах).

7. Інформація про громадян (персональні дані) – відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особу.

8. Конфіденційна інформація – документована інформація, доступ до якої обмежується відповідно до законодавства України.

9. Засоби забезпечення автоматизованих інформаційних систем та їх технологій – програмні, технічні, лінгвістичні, правові, організаційні засоби (програми для електронних обчислювальних машин; засоби обчислювальної техніки і зв'язку; словники, тезауруси і класифікатори; інструкції; схеми та інформація про них, інша експлуатаційна та супровідна документація), що використовуються або створюються при проектуванні інформаційних систем і забезпечують їх експлуатацію.

10. Власник інформаційних ресурсів, інформаційних систем, технологій та засобів їх забезпечення – суб'єкт, в повному обсязі реалізує повноваження володіння, користування, розпорядження зазначеними об'єктами.

11. Власник інформаційних ресурсів, інформаційних технологій і засобів їх забезпечення – суб'єкт, який здійснює володіння і користування зазначеними об'єктами і який реалізує повноваження розпорядження в межах, встановлених Законом.

12. Користувач (споживач) інформації – суб'єкт, який звертається до інформаційної системи або посередника за одержанням необхідної йому інформації і користується нею.

Під поняттям «інформаційний злочин» розуміються суспільно небезпечні дії, заборонені кримінальним законом під загрозою покарання, вчинені в галузі інформаційних технологій.

Основними завданнями фахівця із організації інформаційної безпеки в галузі інформаційних, комп'ютерних технологій є:

- освоєння студентами кваліфікації та навичок визначення основних загроз інформації в комп'ютерних системах і технологіях і мережах;
- освоєння принципів паралельного аналізу цілей і можливостей зловмисника в комп'ютерних системах і технологіях, методів проведення організаційних заходів щодо забезпечення інформаційної безпеки;
- освоєння методів захисту інформації в автоматизованих системах приймання, оброблення, зберігання і розповсюдження інформації в комп'ютерних системах.

1.2. Поняття інформаційної безпеки

Під терміном «інформаційна безпека», згідно Закону України, розуміють стан захищеності інформації, що обробляється засобами обчислювальної техніки або автоматизованої системи, від внутрішніх або зовнішніх загроз: від небажаного її розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати або зниження ступеня доступності інформації, а також її незаконного тиражування, які призводять до матеріального або морального збитку власника або користувача інформації.

Відповідно, під інформаційною безпекою мається на увазі комплекс заходів, що проводяться з метою запобігання від дій загроз безпеки інформації, де загроза є потенційною можливістю порушення безпеки інформації.

Коли говорять про інформаційну безпеку, то мають на увазі широкий спектр проблем: від стихійних лих і проблем з електроживленням до досвідчених зловмисників, які використовують обчислювальні системи для своєї вигоди, або шпигунів, які полюють за державними і комерційними секретами.

Виникнення проблеми забезпечення інформаційної безпеки при підключенні організацій до світових відкритих мереж безпосередньо пов'язано з їх основними перевагами – оперативністю, відкритістю, глобальністю. Без реалізації основних заходів безпеки будь-який користувач має можливість дістатися до будь-якого комп'ютера, щоб отримати доступ до інформації, до мережевих ресурсів або запустити програмний модуль на віддаленому комп'ютері.

Підключення до Internet, використання її служб і сервісів само по собі не створює будь-яких принципово нових проблем в галузі забезпечення інформаційної безпеки, відмінних від тих, які існують при зв'язку комп'ютерних систем по відкритих каналах міжмашинного обміну.

У загальному вигляді основними загрозами інформаційній безпеці при підключенні до Internet є:

- несанкціонований (неавторизований) доступ зовнішніх користувачів мережі Internet до будь-якого виду сервісного обслуговування, що надається легальним користувачам (подібна загроза виникне, якщо користувачі деяких банківських мереж України, яким в Internet відкриті тільки три сервіси – WWW, FTP, e-mail – спробують скористатися сервісом telnet, що дозволяє виконувати на віддаленому комп'ютері команди таким чином, немовби ці користувачі сидять за терміналом, безпосередньо підключеному до комп'ютера);
- доступ до інформації та баз даних організацій без ідентифікації і аутентифікації зовнішнього користувача в мережі,

включаючи проникнення до ресурсів абонентів в абонентських пунктах або на хости з метою несанкціонованого доступу до інформації, її руйнування або спотворення (за визначенням НСД – це доступ до інформації, який здійснюється штатними технічними засобами з порушенням встановлених правил розмежування доступу);

- перенесення (імпорт) в системи і мережі організацій руйнівного програмного забезпечення (ПЗ), яке може мати вигляд вірусів, «троянських коней», «закладок» в тілі електронних повідомлень тощо;
- спотворення (порушення цілісності) ПЗ систем і мереж організацій з метою зміни виконуваних ними функцій, аж до повної дезорганізації їх роботи;
- порушення конфіденційності інформаційного обміну по каналах зв'язку абонентів систем і мереж організацій, для чого ці канали можуть «прослуховуватися» за допомогою спеціальних програмно-апаратних засобів;
- доступ до інформації про топології мереж і використовуваних в них механізми захисту, що полегшує зловмисникам проникнення в мережі.

Результати впливу загроз можуть виражатися в появі збоїв в роботі інформаційних систем організацій, спотворенні або руйнуванні циркулюючої інформації, яка зберігається в них, порушення захисних механізмів систем, що дозволяє здійснити НСД до інформації і контролювати роботу ІС.

Internet в кредитно-фінансовій сфері використовується для взаємного інформаційного обміну між різними суб'єктами, а також для постійного зв'язку між територіально віддаленими підрозділами та філіями. Комп'ютерних злочинів в цій сфері, що здійснюються через Internet, також існує дуже багато. Злочинцям найцікавіша інформація про банківську, комерційну таємницю, таємницю вкладів, відомості про фінансове становище самого банку і його клієнтів, службова інформація, а також інформація, що дозволяє зробити висновки про інвестиційну і кредитну політику конкретного банку і напрямки його подальшого розвитку.

Іншу групу злочинів в Internet – економічних – можна розподілити на два основні класи:

1) порушення авторських та інших суміжних прав – незаконне копіювання та продаж комп'ютерних програм, отриманих з хакерських вузлів; виготовлення піратських копій компакт-дисків; незаконне виготовлення друкованої продукції з використанням комп'ютерних міні-друкарень;

2) безоплатне отримання товарів і послуг (наприклад, телефонних компаній – інструкції як це робити є в журналі Phrack (http://www.phrack.com); модифікація інформації про послуги і їх споживачів в базах даних відповідних компаній шляхом злому захисту комп'ютерних систем; інші види шахрайства – незаконна організація азартних ігор, організація фіктивних контор і т. ін.).

З вищевикладеного випливає, що в Internet виділено три рівні забезпечення інформаційної безпеки, починаючи від простих і переходячи до все більш складних механізмів захисту:

1) безпека обчислювальних платформ (апаратного і програмного забезпечення) мережі або комп'ютера, що рівнозначно забезпечення захисту кожного хоста окремо;

2) безпека окремо взятих мережі або комп'ютера, що визначає політику захисту мережі з контролем мережевого доступу до різних хостів і сервісів;

3) безпеку міжмережевої взаємодії мереж і окремих комп'ютерів, які мають підключення до Internet, що конкретизує заходи і засоби захисту каналів зв'язку між мережами і ПК.

1.3. Поняття, властивості інформації

Інформація – це результат відображення і обробки в людській свідомості різноманіття навколишнього світу, відомості про оточуючих людину предмети, явища природи, діяльність інших людей і т. ін. Однак захисту підлягає та інформація, яка представляє цінність. Цінність визначається виключно здатністю

отримання виграшу: морального, матеріального тощо. Оскільки завжди знаходяться зацікавлені в отриманні такої інформації, то і необхідно вживати заходів щодо її захисту.

Необхідно відзначити, що важливість інформації може бути представлена за категоріями важливості в наступному вигляді:

- життєво важлива інформація – незамінна інформація, наявність якої необхідно для функціонування організації;
- важлива інформація – інформація, яка може бути замінена або відновлена, але процес відновлення утруднений і пов'язаний з великими витратами;
- корисна інформація – інформація, яку важко відновити, але організація може ефективно функціонувати і без неї;
- несуттєва інформація – інформація, яка не потрібна організації.

Цей принцип узгоджується з принципом секретності. Під цим принципом розуміється – адміністративна або законодавча міра, відповідна мірі відповідальності особи за витік інформації і втрату конкретної, з урахуванням державних, військово-стратегічних, комерційних, службових або приватних інтересів.

Види і форми подання інформації. Інформація в комп'ютерних системах і технологіях, як правило, представляється у вигляді: букв, символів, цифр; слів; тексту; малюнків; формул; графіків; таблиць; планів; креслень; карт географічних, топологічних, технологічних; алгоритми і т. ін., що можуть бути представлені у вигляді: постійних змінних даних; команд; повідомлень; довідок; рішень; наказів; розпоряджень; завдань; звітів; відомостей; інструкцій; коментарів; листів і записок; телеграм; чеків; масивів; файлів тощо.

Машинне подання інформації. Інформація, зафіксована в матеріальній формі, називається повідомленням. Повідомлення можуть бути безперервними і дискретними (цифровими).

Безперервне повідомлення – надання інформації деякої фізичної величини (електричний струм, напруга тощо).

Дискретне повідомлення – подання інформації у вигляді фіксованого набору окремих елементів в дискретні моменти часу. У

комп'ютерних системах і технологіях, які використовують цифрове представлення інформації називають цифровими системами.

Елементи, з яких складається дискретне повідомлення, називають буквами або символами. Набір цих букв – алфавіт. Число символів в алфавіті – обсяг алфавіту. Обсяг алфавіту визначає кількість інформації, що доставляється одним символом повідомлення.

Фізичне представлення інформації і процеси її обробки. Неодмінна вимога до фізичних аналогів двійкового представлення алфавіту – надійність розпізнавання двох різних значень сигналу «0» або «1».

У цифрових системах застосовують три способи фізичного представлення інформації: потенційний, імпульсний і динамічний у вигляді послідовного або паралельним коду. При використанні послідовного коду комп'ютерні системи працюють повільно, при паралельному поданні швидше, але при цьому потрібні значні витрати на апаратне оснащення.

Інформація в КС реалізується через процеси введення, зберігання, оброблення і виведення. Введення інформації в КС здійснюється з фізичних носіїв інформації: паперових, магнітних, оптичних, електронних, клавіатури, спеціальних пультів і т. ін.

Зберігання інформації проводиться на запам'ятовуючих пристроях: короткочасне – в ОЗП і різних регістрах пам'яті; довготривале зберігання – в зовнішніх запам'ятовуючих пристроях, виконаних на електронних носіях, магнітних стрічках, барабанах, дисках тощо.

Виведення інформації проводиться на зовнішні пристрої зв'язку і реєстрації інформації без її візуального відображення (на зазначені вище носії інформації), пристрої друку, індикаторні табло тощо. Вибір методів виведення інформації визначається можливостями КС.

Інформаційні процеси в системах обробки даних може бути умовно визначені на три групи:

- інформаційно-довідкове забезпечення посадових осіб органів управління;

- інформаційне забезпечення розрахункових завдань;
- обслуговування інформаційної бази КС.

Ці процеси реалізують посадові особи органів управління та обслуговуючий персонал за допомогою апаратних засобів автоматизації і зв'язку.

Інформація як об'єкт права власності. Велика проблема даного питання полягає в тому, що захист підлягає не сама інформація, а права власності на інформації. Історично склалося так, що об'єктом власності завжди були матеріальні речі. Інформація – це ідеальна категорія, але завжди пов'язана з матеріальними предметами – носіями інформації: мозок людини, книга, диски, флешки тощо Ці об'єкти мають всі властивості товарів, з тією лише різницею, що подібний товар може копіюватися, поширюватися. Таким чином, не зважаючи на ряд особливостей, інформація повинна бути об'єктом власності. Юридично це закріплено в законах України, де визначено, що інформаційні ресурси, окремі документи або масиви документів, є об'єктами відносин фізичних та юридичних осіб, що підлягають обліку та захисту як матеріальне майно власника.

Інформація – комерційна таємниця. Захист інформації та прав суб'єктів у галузі інформаційних процесів регулюється законами України. Перелік відомостей що становлять комерційну таємницю згруповані за тематичними групами:

1. Відомості про фінансову діяльність.
2. Інформація про ринок.
3. Відомості про виробництво і продукції.
4. Відомості про наукові розробки.
5. Відомості про систему матеріально-технічного забезпечення.
6. Відомості про персонал підприємства.
7. Відомості про принципи управління підприємством.
8. Інші відомості (елементи систем безпеки, принципи захисту комерційної таємниці).

1.4. Законодавство про інформаційні правовідносини

Вся сукупність злочинів у сфері комп'ютерної інформації може бути представлена у вигляді таблиці 2.1.

Табл. 2.1

Види суб'єктів	**Вид дій**	**Види об'єктів дії**	**Види місце-знаходження об'єктів**	**Види наслідків**
Особа, яка має доступ до ЕОМ	Неправомірний доступ	Під охороною законом комп'ютерна інформація	ЕОМ	Знищення інформації
	Створення шкідливих програм	Інформація	Система ЕОМ	Блокування інформації
	Використання шкідливих програм	Програми	Мережа ЕОМ	Модифі-кація інформації
	Поширення шкідливих програм	Під охороною законом інформація (ЕОМ)	Машинний носій	Копіювання інформації
	Внесення змін до існуючих програми	Шкідливі програми		Порушення роботи ЕОМ
	Порушення правил експлуатації ЕОМ			

Основні законодавчі акти, що регулюють інформаційні відносини в галузі комп'ютерних злочинів представлені такими законами.

Закон України «Про правову охорону програм для електронних обчислювальних машин і баз даних». Метою даного закону є активізація та стимулювання вітчизняних розробників програмних засобів в галузі інформаційних технологій.

Закон України «Про правову охорону топологій інтегральних мікросхем». Цей закон регулює діяльність у галузі захисту прав авторів і розробників програмно-технічного забезпечення. У законі зафіксовано поняття і правові конструкції, що відображають уявлення законодавця про елементи, що охороняється у цій сфері, юридичні визначення програми для ЕОМ і бази даних. Програма для ЕОМ розглядається як форма представлення сукупності даних і команд. База даних розглядається як об'єктивна форма представлення та організації сукупності даних (наприклад, статей, розрахунків), систематизованих таким чином, щоб ці дані могли бути знайдені і оброблені на ЕОМ.

Закон України «Про авторське право і суміжні права» регулює відносини, що виникають у зв'язку зі створенням і використанням творів науки, літератури і мистецтва, фонограм, виконань, постановок, передач організацій ефірного та кабельного мовлення (суміжні права).

Закон України «Про державну таємницю» регулює відносини, що виникають у зв'язку з віднесенням інформації до державної таємниці, їх розсекречення та захистом в інтересах забезпечення безпеки України. Законом визначено поняття державної таємниці як захищені державою відомості в галузі військової, зовнішньополітичної, економічної, розвідувальної та оперативно-розшукової діяльності, поширення яких може завдати шкоди безпеці України. У закон введено визначення носіїв відомостей, що становлять державну таємницю і засоби інформаційної безпеки. До носіїв відомостей віднесені матеріальні об'єкти, в тому числі фізичні поля в яких відомості, що становлять державну таємницю, знаходять своє відображення у вигляді символів, образів, сигналів,

технічних рішень і процесів. До засобів захисту відносяться технічні, криптографічні, програмні та інші засоби, призначені для захисту відомостей, що становлять державну таємницю, а також засоби контролю ефективності захисту інформації. Важливим є і визначення доступу до відомостей, що становлять державну таємницю.

Закон України «Про обов'язковий примірник документів» визначає поняття документа. Під документом розуміється матеріальний об'єкт із зафіксованою на ньому інформацією у вигляді тексту, звукозапису або зображення, призначений для передавання в часі і просторі з метою зберігання та громадського використання. У 5 статті цього закону відображена класифікація документів.

Закон України «Про зв'язок» встановив правову основу діяльності в галузі зв'язку, визначив повноваження органів державної влади з регулювання зазначеної діяльності, а також права та обов'язки фізичних осіб, які беруть участь у зазначеній діяльності або користуються послугами зв'язку.

Закон України «Про захист інформації в автоматизованих системах» регулює відносини, що виникають при: формуванні та використанні інформаційних ресурсів на основі створення, збирання, оброблення, накопичення, зберігання, пошуку, розповсюдження і надання споживачеві документованої інформації; створенні та використанні інформаційних технологій і засобів їх забезпечення; інформаційної безпеки, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації.

Закон України «Про участь у міжнародному інформаційному обміні» створює умови для ефективної участі України в міжнародному обміні в межах світового інформаційного простору, захист інтересів України та муніципальних утворень при міжнародному обміні, захист інтересів, прав і свобод фізичних і юридичних осіб при міжнародному інформаційному обміні.

1.5. Класифікація комп'ютерних систем

Класифікація комп'ютерних систем проводиться за такими ознаками:

- за способом побудови;
- за функціональним призначенням;
- за розміщенням інформації в мережі;
- за числом головних обчислювальних машин (ГОМ)
- за типом використовуваних ЕОМ
- за методом передавання даних
- за реалізацією топології з'єднання комп'ютерних систем в мережі.

За способом побудови, розрізняють на зосереджені і розподілені КС (рис. 1.1).

За функціональним призначенням розрізняють комп'ютерні системи: автоматизованої обробки даних і автоматизовані системи контролю управління виробництвом, технологічними процесами і об'єктами. Автоматизовані системи обробки даних розрізняють на: інформаційні, які надають користувачу в основному інформаційне обслуговування; обчислювальні, що виконують головним чином рішення задач з обміну даними та програмами між ЕОМ мережі, і змішані інформаційно-обчислювальні.

За розміщення інформації в системі розподіляють на КС з централізованим банком даних, який формується в одному з вузлів системи, і з розподіленим банком даних, що складається з окремих локальних банків, розташованих у вузлах системи.

За ступенем територіального розосередження можна виділити великомасштабні, або глобальні, обчислювальні системи, що охоплюють територію країни, декількох країн з відстанями між вузлами мережі, що вимірюються тисячами кілометрів; регіональні системи, що охоплюють певні регіони – місто, район, область і т.ін.; локальні обчислювальні системи з максимальною відстанню між вузлами системи не більше кількох кілометрів.

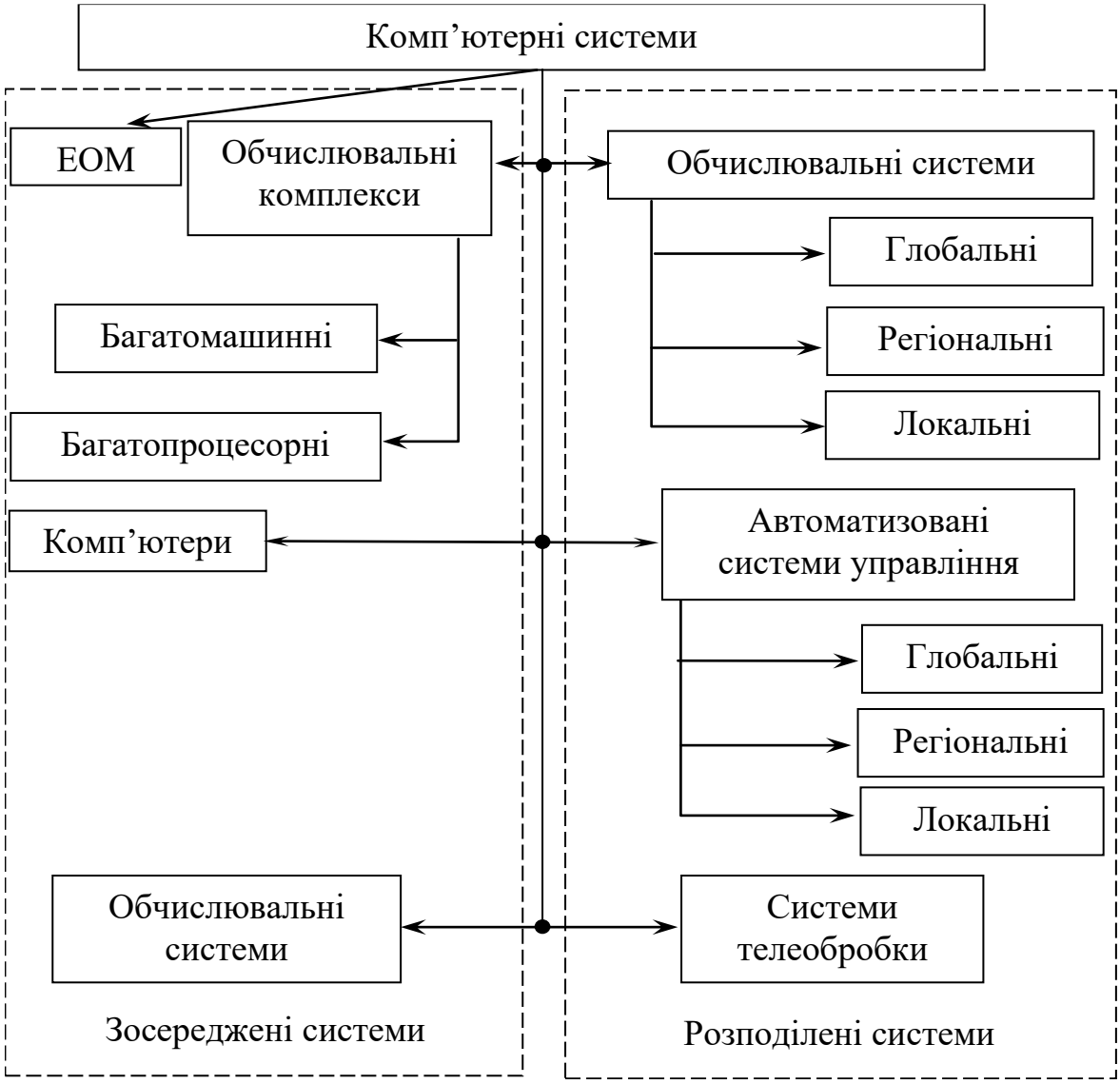


Рис. 1.1. Класифікація комп’ютерних систем за способом побудови

За кількістю ГОМ слід розрізняти мережі з декількома і з одною ГОМ. Останні відносяться до обчислювальних систем з телеобробки, які являють собою комплекси, що складаються з обчислювальної машини і віддалених абонентських пунктів (АП), пов’язаних з допомогою каналів і апаратури передавання даних.

За типом використовуваних ЕОМ виділяють однорідні мережі, що містять програмно-сумісні машини, і неоднорідні, якщо машини мережі програмно несумісні. На практиці мережі часто є неоднорідними.

За методом передавання даних розрізняють обчислювальні мережі з комутацією каналів, з комутацією повідомлень, з комутацією пакетів і зі змішаною комутацією. Для сучасних комп'ютерних систем і мереж характерно використання комутації пакетів.

Комутація пакетів є розвитком методу комутації повідомлень. Вона дозволяє домогтися подальшого збільшення пропускної здатності мережі, швидкості і надійності передавання даних.

Повідомлення, що поступає від абонента розбивається на пакети, які мають фіксовану довжину, наприклад 1 Кбайт. Пакети наділяються службовою інформацією-заголовком, що вказує адресу пункту відправлення, адресу пункту призначення і номер пакета в повідомленні.

В системі передавання даних між абонентами з комутацією пакетів використовуються два способи передачі: дейтаграммний і віртуальний.

Дейтаграммний спосіб – це передавання даних окремих, не пов'язаних між собою пакетів. Важливою перевагою дейтаграммного способу комутації пакетів є можливість одночасної передачі пакетів одного і того ж повідомлення різними маршрутами, що зменшує час і збільшує надійність передавання повідомлення. При передачі короткими пакетами зменшуються ймовірність появи помилок і час зайнятості каналів повторними передачами. Однак при цьому спостерігаються випадки обгону повідомлень. Прив'язка повідомлень до часу їх видачі та нумерація дозволяють це виявити, але цей спосіб не гарантує черговість і надійність доставки пакетів.

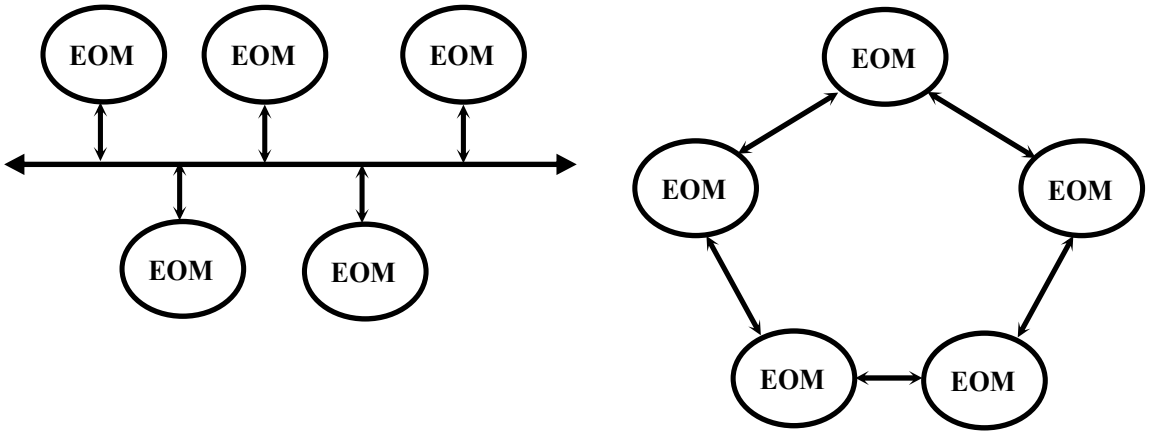
Віртуальний спосіб – передавання даних у вигляді послідовностей пов'язаних у ланцюжки пакетів. Організація віртуального каналу між двома процесами рівносильна виділенню їм дуплексного каналу зв'язку, за яким дані передаються в їх природній послідовності. Віртуальний канал зберігає всі вищеописані переваги комутації пакетів щодо швидкості передавання і мультиплексування, але вимагає попередньої процедури встановлення з'єднань. Після закінчення сеансу зв'язку

канал розпадається і повертає ресурси для встановлення нових віртуальних з'єднань.

Важливою ознакою класифікації комп'ютерних систем є реалізація топології їх з'єднання в мережі. Топологічна структура мережі значно впливає на її пропускну здатність, стійкість до відмов її обладнання, на логічні можливості і вартість. В наш час спостерігається велика різноманітність у топологічних структурах обчислювальних мереж (рис. 1.2).

Топологія великих комп'ютерних систем може являти собою комбінацію декількох топологічних рішень.

В обчислювальних мережах (системах) її абоненти оснащуються спеціальними програмними засобами для мережевої обробки даних. До програмних засобів пред'являються вимоги щодо збереження працездатності мережі при зміні її структури, при відмовах окремих ЕОМ, каналів і вузлів зв'язку, а також забезпечення можливості роботи ЕОМ з терміналами різних типів і взаємодії різнотипного обладнання.



а) б)

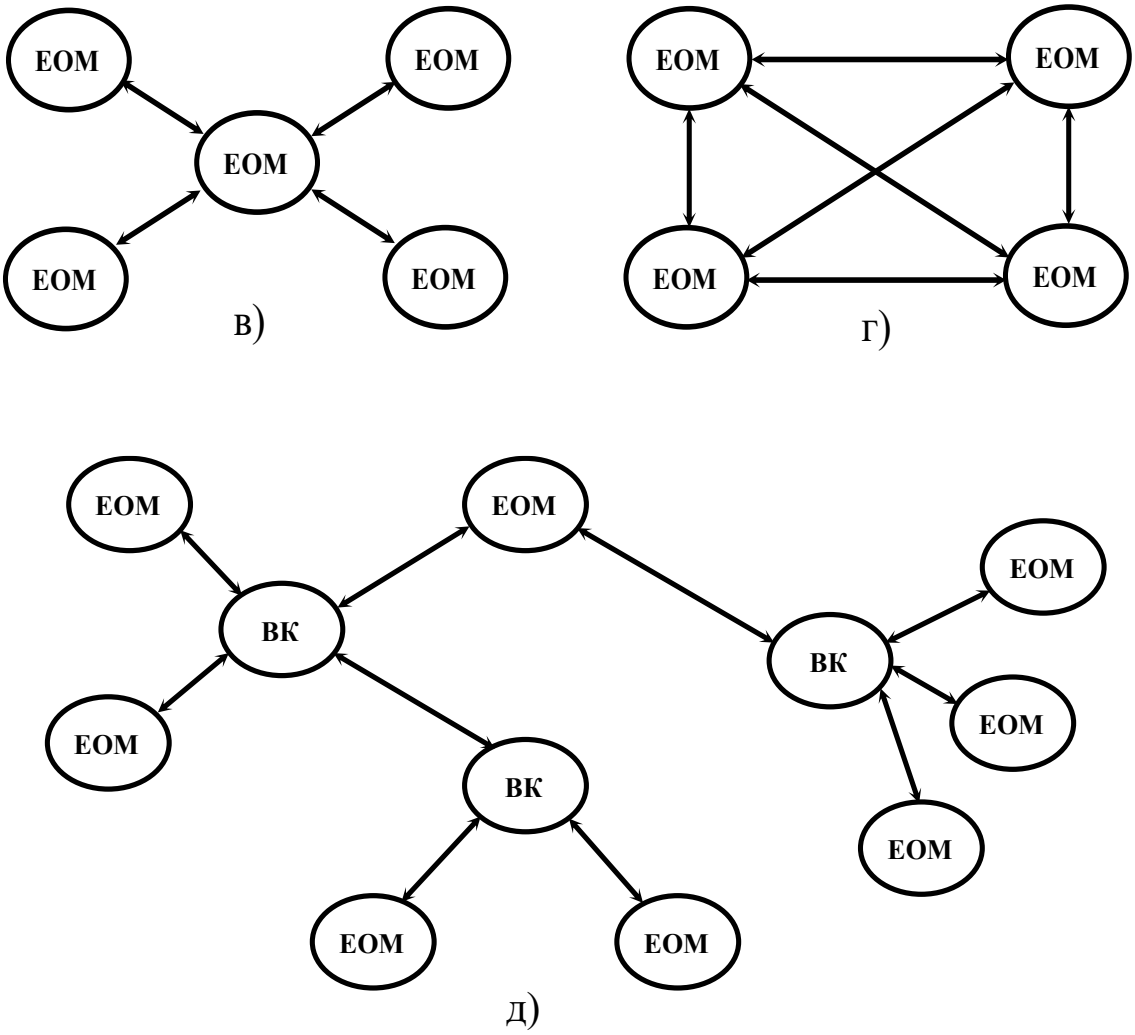


Рис. 1.2. Топологічні структури комп'ютерних обчислювальних мереж (а – одинарна багатоточкова лінія типу «шина»; б – мережа типу «кільце»; в – зіркоподібна мережа типу «зірка»; г – повнозв'язана мережа ; д – деревоподібна мережа)

1.6. Об'єкти захисту в персональних комп'ютерах, інформаційних системах і технологіях

При аналізі та оцінюванні міцності інформаційної безпеки необхідне знання об'єкта захисту, основ побудови комп'ютерних систем, перелік їх основних компонент. Основою комп'ютерних систем є персональний комп'ютер.

Класична структурна схема комп'ютера, представлена на рис. 1.3, містить: арифметично-логічний пристрій, пам'ять, управляючий пристрій, пристрій введення-виведення, клавіатуру, операційну систему, комплект програм технічного обслуговування, пакети прикладних програм.

Арифметично-логічний пристрій (АЛП) здійснює арифметичні і логічні перетворення над машинними словами, тобто кодами певної довжини, що являють собою числа або інший вид інформації.

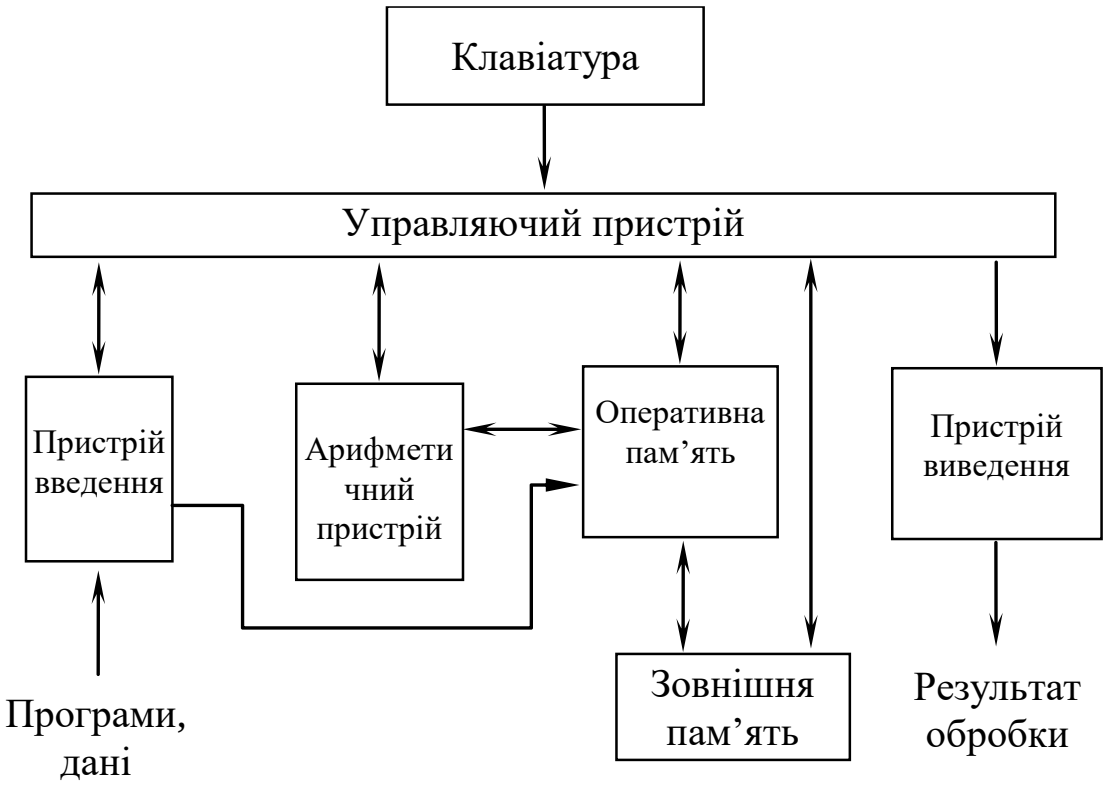


Рис. 1.3. Структурна схема персонального комп'ютера

Пам'ять – зберігає інформацію, що передається з інших пристроїв в тому числі ззовні через пристрій введення і виведення інформації, необхідну для протікання обчислювального процесу.

Управляючий пристрій – необхідний для забезпечення автоматичного управління обчислювального процесу. Виконує окремі операції за заданим алгоритмом розв'язання задачі чисельним методом. Всі операції проводяться відповідно до програми, що складається з окремих команд.

Пристрій виведення служить для видачі з машини інформації.

Клавіатура необхідна для забезпечення ручного введення, запуску, зупинки та зміни алгоритму або програми роботи комп'ютера. Система програмного забезпечення підтримується за допомогою операційної системи. Структура програмного забезпечення представлена на рис. 1.4.

Операційні системи призначені для ефективного управління обчислювальним процесом, планування і автоматизації процесу. Оператори, що працюють за комп'ютером, не мають прямого доступу до пристроїв ЕОМ. Зв'язок операторів з комп'ютером проводиться за допомогою операційної системи, що підтримує певний рівень спілкування людини з машиною. Рівень спілкування визначається рівнем мови, на якому воно відбувається (Сі ++, Паскаль та ін.).

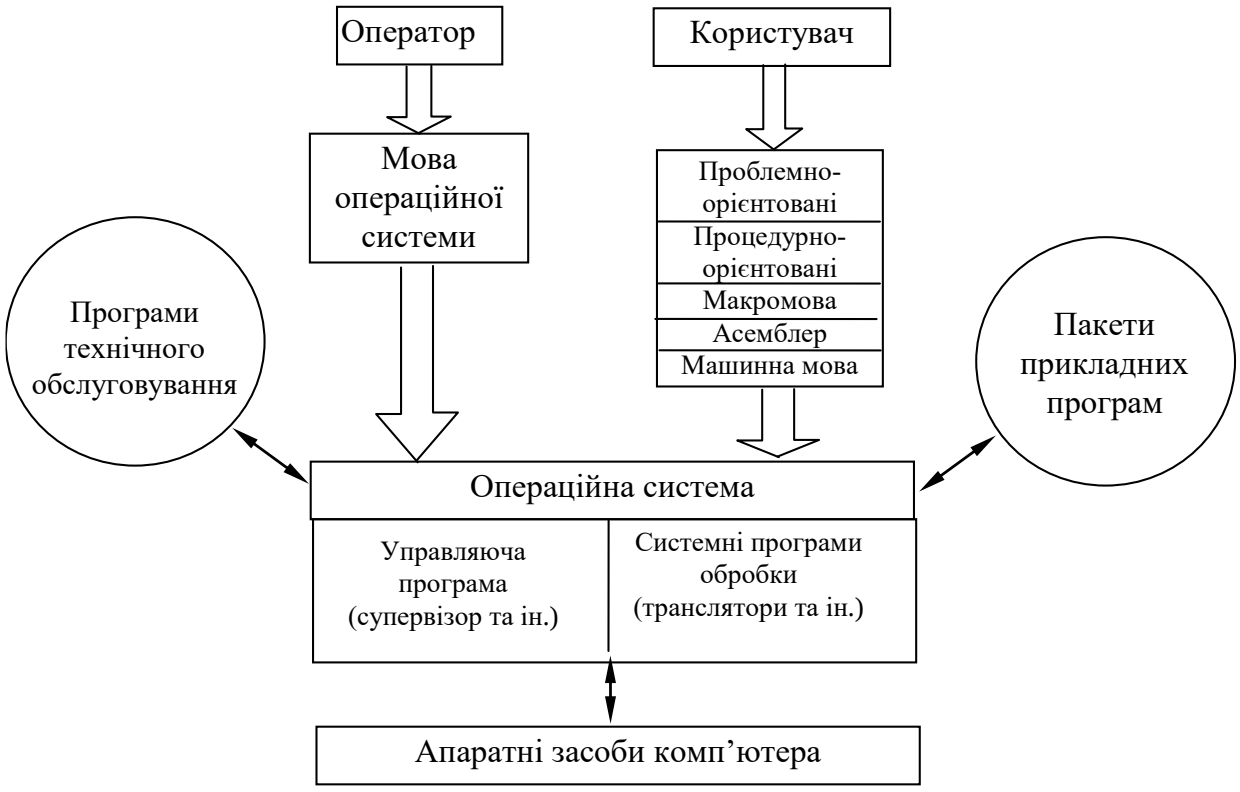


Рис. 1.4. Структурна схема програмного забезпечення персонального комп'ютера

Комплект програм технічного обслуговування призначені для зменшення трудомісткості експлуатації комп’ютера і містить програми перевірки працездатності машини і окремих її пристроїв і їх діагностики.

Пакети прикладних програм призначені для вирішення конкретних завдань (інженерно-технічних, планово-економічних тощо), а також для розширення функцій операційних систем (управління базами даних, управління режимами телеобробки та ін.).

Тема 2. Аналіз потенційних загроз безпеці інформації в комп'ютерних системах і технологіях

2.1. Постановка завдання аналізу потенційних загроз

Дослідження і аналіз випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на ненавмисні і навмисні. При цьому навмисні загрози, як правило, в результаті систематичного застосування можуть бути приведені через випадкові, шляхом довготривалої масивної атаки несанкціонованими запитами або вірусами.

Наслідки, до яких призводить реалізація загроз: руйнування (втрата) інформації, модифікація (зміна на помилкову, яка коректна за формою і змістом, але має інший зміст) і витоку інформації (несанкціоноване копіювання з метою розкрадання). Для створення засобів інформаційної безпеки необхідно визначити природу загроз і шляхів їх можливого прояву в КС. Для вирішення поставленого завдання все різноманіття загроз і шляхів їх впливу приведемо до найпростіших видів і форм, які були б адекватні їх множині в КС.

Дослідження і оцінювання рівня інформаційної безпеки зводиться до класифікації потенційних загроз, які можуть бути визначені як випадкові загрози і навмисні загрози.

2.1.1. Випадкові загрози

При дослідженні досвіду проектування відзначається, що інформація опиняється під загрозою в процесі введення, зберігання, оброблення, виведення і передавання. В результаті таких дій на апаратному рівні відбуваються фізичні зміни рівнів сигналів у

цифрових кодах, що несуть інформацію. При цьому спостерігається зміна «1» на «0» або «0» на «1». Якщо засоби функціонального впливу здатні це виявити (наприклад, виявлення одноразової помилки), то проводиться бракування даного коду, а пристрій або виріб визнається несправним. В іншому випадку відбувається подальша зміна інформації, що передається.

Якщо зміни відбуваються на програмному рівні, в результаті випадкових впливів можлива зміна алгоритму оброблення інформації, що веде до непередбачуваних наслідків. При програмних помилках можуть підключатися пристрої введення-виведення і передавання їх на заборонені пристрої.

Причинами випадкового впливу можуть бути:

- відмови і збої апаратури;
- перешкоди на лініях зв’язку від впливів зовнішнього середовища;
- помилки людини як ланки системи;
- схемні і схемотехнічні помилки розробників;
- структурні, алгоритмічні та програмні помилки;
- аварійні ситуації та інші впливи.

Частота відмов і збоїв апаратури збільшується, якщо на етапі проектування не враховують перераховані вище фактори виникнення випадкових загроз. Перешкоди, що виникають в лініях зв’язку, залежать від вибору технічних засобів і їх розміщення відносно один одного і по відношенню до інших комп’ютерних систем. В процесі проектування комп’ютерних систем на надійність впливає кваліфікація розробників, умови їх роботи, наявність досвіду та ін.

На етапі виготовлення і випробувань на якість вхідної в комп’ютерну систему апаратури впливають повнота і якість технічної документації, за якою вона виготовляється і технологічна дисципліна на етапі виготовлення.

До помилок людини як ланки системи слід віднести помилки як джерела інформації, людини – неправильні дії роботи обслуговуючого персоналу і помилки людини, як ланки, що

приймає рішення. Помилки людини поділяються на логічні (неправильні рішення), сенсорні (неправильне сприйняття оператором інформації) і оперативні, або моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатися в межах від 1-2% до 15-40% і вище загального числа операцій, які виконуються при вирішенні завдань. Інтенсивність помилок залежить від стану людини і характеризується його стомлюваністю, психологічними параметрами, віком, чутливістю до зміни навколишнього середовища, залежністю якості роботи від фізичного стану, емоційністю.

Для розрахунку достовірності вихідної інформації важливі статистичні дані за рівнем помилок людини як ланки системи. Як показує аналіз роботи систем, інтенсивність помилок людини становить $2 \cdot 10^{-2} – 4 \cdot 10^{-3}$. Помилки людини як ланки системи, яка приймає рішення, визначаються неповною адекватністю уявлення людиною реальної ситуації і створення спрощеної моделі ситуації.

До загроз випадкового характеру слід віднести також аварійні ситуації, які можуть виникнути на об’єкті, де розміщена комп’ютерна система. До таких аварійних ситуацій слід віднести:

- відмову функціонування комп’ютерної системи в цілому в результаті відключення електроживлення та освітлення;
- стихійні лиха: пожежа, повінь тощо;
- відмова системи життєзабезпечення на об’єкті експлуатації комп’ютерної системи.

Імовірність цих подій напряму пов’язана з правильним розміщенням, включаючи географічне розміщення та організацією протипожежних заходів.

2.1.2. Навмисні загрози

Навмисні загрози пов’язані з діями людини, причинами яких можуть бути певні невдоволення своєю життєвою ситуацією, матеріальним інтересом або простою розвагою. Потенційні загрози з цього боку слід розглядати тільки в технічному аспекті. Для

постановки завдання захисту інформації необхідний аналіз об’єкта захисту на предмет введення-виведення, зберігання та передавання інформації і можливостей порушника з доступу при відсутності засобів захисту. Для комп’ютерних систем характерні наступні штатні канали доступу до інформації:

- термінали користувачів та адміністратора системи;
- термінал оператора функціонального контролю (оператора системи);
- засоби відображення інформації;
- засоби документування інформації;
- засоби завантаження програмного забезпечення в КС;
- носії інформації (ОЗП, ДЗП, паперові носії);
- зовнішні канали зв’язку.

Для реалізації НСД порушник може отримати доступ до апаратури, програмного забезпечення і здійснити розкрадання, модифікацію, руйнування інформації:

- при їх використанні законними користувачами не за призначенням і за межами своїх повноважень всіх перерахованих штатних засобів;
- використання сторонніми особами всі перераховані штатні засоби;

а також такими технічними каналами через:

- технологічні пульти;
- внутрішній монтаж апаратури;
- лінії зв’язку між апаратними засобами даної комп’ютерної системи;
- побічне електромагнітне випромінювання інформації засобами даної комп’ютерної системи;
- побічні наведення інформації по мережі електроживлення і заземлення апаратури;
- побічні наведення інформації на допоміжних і сторонніх комунікаціях;

• відходи оброблення інформації у вигляді паперових і магнітних носіїв, кинутих у сміттєву корзину.

До складу апаратури комп'ютерної системи входять персональний комп'ютер, принтер, цифрові табло, телефонні апарати, ксерокс, сканер тощо.

При наявності вільного доступу, при відсутності службового персоналу порушник може спостерігати інформацію на пристроях відображення, викрасти інформацію, як на паперових, так і на магнітних носіях. Найбільш небезпечним є незаконне завантаження нештатного програмного продукту типу «троянського коня», вірусу тощо. Якщо порушник є законним користувачем, то дана небезпека зростає багаторазово, так як можливе знімання інформації, цінність якої виходить за межі його повноважень і доступу. При неоднозначній ідентифікації інформаційних ресурсів порушник має вільний доступ до системної бібліотеки, що дозволяє забезпечити вільний доступ до всієї інформації наявної в даній комп'ютерній системі.

При технічному обслуговуванні (профілактиці і ремонті) апаратури можуть бути виявлені залишки видаленої інформації. При звичайній процедурі видалення файлів на диску залишаються фрагменти видаленої інформації. При транспортуванні носіїв може бути здійснене її перехоплення сторонніми особами з метою отримання секретної інформації.

При аналізі можливих шляхів доступу до інформації слід відзначити загрози, яким можуть піддаватися канали та комп'ютерні мережі (рис. 2.1).

На схемі показано, що порушник може підключитися на ділянці В і працювати під уявним шлюзом, контролюючи тим самим весь інфопотік і здійснювати як пасивне, так і активне його перехоплення.

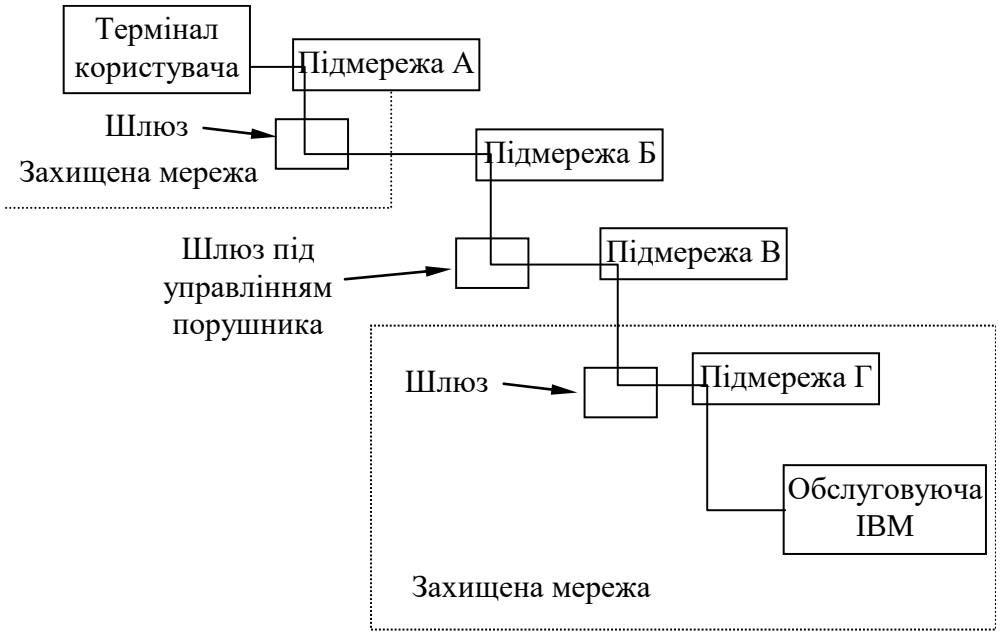


Рис. 2.1. Схема можливого підключення порушника до мережі комп'ютерної системи

При пасивному перехопленні порушник стежить тільки за потоком інформації, розкриваючи зміст повідомлень з визначенням довжини переданих повідомлень, частот їх передавання з метою аналізу потоку даних.

При активному перехопленні порушник має можливість модифікувати або вводить дезінформацію, затримку повідомлень. Подібні порушення кваліфікується як зміна потоку і змісту повідомлень.

Аналіз загроз інформаційним процесам дає можливість визначити п'ять основних видів загроз:

1) розкриття змісту повідомлень, що передаються;

2) аналіз трафіку, що дозволяє визначити відправника і одержувача;

3) зміна потоку повідомлень, що може привести до порушення режиму роботи будь-якого об'єкта, керованого віддаленим комп'ютером;

4) неправомірну відмову в наданні послуг;

5) несанкціоноване встановлення з'єднань.

Усі перераховані визначення класифікації не суперечать принципу розподілу на загрози: модифікації і втрати інформації.

У КС і технологіях порушник може застосувати такі стратегії:

- отримати несанкціонований доступ;
- видати себе за іншого користувача і скористатися його повноваженнями;
- відмовитися від факту формування переданої інформації;
- стверджувати, що інформація отримана від деякого користувача, хоча вона сформована ним самим;
- стверджувати, що інформації передана користувачеві, насправді вона ним не була відправлена;
- відмовитися від факту отримання інформації;
- незаконно розширити свої повноваження;
- незаконно змінити повноваження інших користувачів;
- приховати факт наявності деякої інформації в іншій інформації (приховане передавання однієї інформації в змісті іншої);
- підключитися до лінії зв'язку між іншими користувачами в якості активного ретранслятора;
- вивчити, хто і коли і до якої інформації отримує доступ;
- заявити про сумнівність протоколу забезпечення інформацією через розкриття деякої інформації, яка повинна бути секретною;
- модифікувати ПЗ шляхом додавання нових функцій;
- навмисно змінити протокол обміну інформацією з метою його порушення або підриву довіри до нього;
- перешкодити обміну сполучення між іншими користувачами.

Таким чином, дуже важливо визначити, кого вважати порушником, бо це може бути не тільки стороння особа, а і законний користувач.

Велику свободу дії для порушників має мережа Internet. У таблиці 2.1 представлені ймовірності прояви загроз інформаційній безпеці в Internet.

Таблиця 2.1

Загрози інформаційній безпеці в Internet

Загрози	Ймовірність Прояву
Недбалість	0,188
Піратство	0,166
Неточна або застаріла інформація	0,159
Витік даних	0,159
«Жарти» над колегами	0,150
Спостереження за випромінюванням	0,133
Умисні пошкодження даних і програм	0,129
Порушення аутентифікації	0,129
Перевантаження	0,119
Неправильна маршрутизація	0,106
Апаратні збої	0,090
Спотворення	0,080
Мережеві аналізатори	0,074
Шахрайство	0,058
Пожежі та інші стихійні лиха	0,043
Підробка	0,033
«Логічні бомби»	0,032
Крадіжка	0,032
Блокування інформації	0,016
«Потаємні ходи і лазівки»	0,010

Можливі шляхи реалізації загроз потенційними порушниками наведені в таблиці 2.2.

Таблиця 2.2

Матриця загроз інформації

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	НСД – підключення; використання ресурсів; розкрадання носіїв	НСД – підключення; використання ресурсів; модифікація, зміна режимів	НСД – зміна режимів; виведення з ладу; руйнування
Програмне забезпечення	НСД – копіювання; розкрадання; перехоплення	НСД, впровадження «троянського коня», «вірусів», «хробаків»	НСД – спотворення; видалення; підміна
Дані	НСД – копіювання; розкрадання; перехоплення	НСД – спотворення; модифікація	НСД – спотворення; видалення; підміна
Персонал	Розголошення; передача відомостей про захист; недбалість	«Маскарад»; вербування; підкуп персоналу	Відхід з робочого місця; фізичне усунення

Слід також зазначити, що завдання захисту від порушників умовно можна розділити на рівень призначений для користувача та рівень елементів і компонентів комп'ютерної системи.

При аналізі міцності інформаційної безпеки необхідно враховувати також рівень довіри між користувачами.

2.2. Аналіз електромагнітних випромінювань і наведень в комп'ютерних системах

2.2.1. Характеристики випромінювання протоколів обміну

Відомо, що спектр періодичного сигналу має дискретний характер, тобто визначений набором амплітуд окремих гармонійних складових, частота яких кратна частоті сигналу. Тому використання в протоколах обміну імпульсних сигналів прямокутної форми і високоякісної комутації в апаратної частини засобів захисту інформації (ЗЗІ) призводить до того, що в спектр випромінювань входять різні компоненти (аж до надвисоких частот). Вимірювання свідчать, що напруженість електричного поля випромінювання протоколів обміну досягає 25 дБ і вище – до частот в сотні МГц.

Таблиця 2.3

Нормовані величини випромінювання

Частота випромінювання, МГц	**Відносна напруженість електричного поля, дБ**	**Частота випромінювання F, МГц**	**Відносна напруженість електричного поля, дБ**
1,08	13	6,2	17
1,35	13	10,15	25
2,05	13	18,2	25
2,8	23	27,1	20
3,6	20	54,6	23
5,13	25	135,2	24

Як приклад у таблиці 2.3 наведені дані вимірювань нормованої величини випромінювання сигналів протоколу обміну

контролера ЗЗІ, вбудованого в комп'ютер, з електронним ідентифікатором DS.

Параметри знімаються на відстані одного метра від об'єкта. За допомогою осцилографа, підключеного до виходу селективних приймачів, контролюється вид сигналів. Для інших систем захисту інформації або контролю доступу (наприклад тих, які використовують в якості пристроїв аутентифікації користувачі Proxi-карти) значення відносної напруженості поля можуть значно перевищувати величини, зазначені в таблиці 2.3.

Розрахунки показують, що з урахуванням мінімальної тривалості імпульсних сигналів обміну приймач, призначений для знімання інформації і її повного відновлення, при співвідношенні сигнал – шум 10 дБ, повинен володіти смугою пропускання не менше 40 кГц і чутливістю приймача 0,15-0,2 мкв. Вказані параметри мають багато пристроїв, що пропонуються на українському ринку.

2.2.2. Аналіз спектру випромінювання протоколу обміну

Не заглиблюючись у питання конкретних засобів захисту, систем контролю доступу, електронних ідентифікаторів і їхніх конструктивних особливостей, розглянемо можливі способи забезпечення надійного захисту протоколів обміну ЗЗІ від «злому» шляхом перехоплення і подальшого аналізу побічних електромагнітних випромінювань. Це, перш за все, використання в протоколах обміну сигналів у вигляді псевдовипадкових імпульсних послідовностей (ІП), що являють собою дискретні стаціонарні процеси з розподілом окремих параметрів (незалежних між собою) за тим чи іншим заздалегідь заданим принципом. Такий аналіз параметрів імпульсної послідовності в будь-якому інтервалі часу дозволяє ідентифікувати користувача. Після кожного обміну між засобом ідентифікації і апаратною частиною ЗЗІ необхідна зміна і запис характеристик послідовності розподілу випадкових параметрів імпульсної послідовності. Це дозволить максимально

знизити можливість «злому» системи шляхом перехоплення і аналізу побічного електромагнітного випромінювання і наведень (ПЕМВН). У якості параметрів імпульсної послідовності в цифрових схемах оброблення сигналів використовуються: тривалість окремих імпульсів, часові відстані між імпульсами або комбінації тривалості і відстані.

При цифровій обробці попередньо спотворених імпульсних послідовностей для відновлення вихідної форми цифрових сигналів в апаратній частині засобів захисту використовуються програмовані цифрові фільтри з максимальною розрядністю, співрозмірною з шумами каналу зв'язку. За допомогою програмованих попередніх спотворень задається певна швидкість зміни огинаючої імпульсів цифрових сигналів, відповідно, фіксування рівнів позасмугових випромінювань. Максимальна ймовірність ідентифікації при мінімальних часових інтервалах аналізу сигналу і витрати пам'яті комп'ютера досягається шляхом застосування інтерполяційного методу звернення до табличного ПЗП, який містить інформацію про форму імпульсу, що генерується.

Ідентифікація користувача у цьому випадку заснована на фільтрації сигналу на вході системи і аналізі інформаційного імпульсу. При побудові даного способу захисту враховується необхідність генерації шумового сигналу в досить широкому діапазоні частот і відновлення вихідної форми відеосигналів після фільтрації шумової перешкоди.

2.2.3. Аналіз спектру випромінювання наведень обладнанням комп'ютерної системи

Поряд із загальновідомими каналами витоку інформації (несанкціонований доступ, підключення до ліній зв'язку або пристроїв обчислювальної техніки тощо), можливий і радіотехнічний канал витоку, коли інформація може бути перехоплена прийомом сигналів побічного електромагнітного

випромінювання і наведень (ПЕМВН), що виникає при функціонуванні пристроїв обчислювальної техніки. Одним з напрямків забезпечення інформаційної безпеки є захист інформаційних процесів та інформації, що знімається за рахунок ПЕМВН. Для створення найпростішої системи відновлення інформації за рахунок прийому ПЕМВН необхідно знати, частоти випромінювання, потужність і смугу прийнятих корисних сигналів, необхідне посилення приймача і антени.

Вимірювання в приміщенні при відстані від прийомної антени до комп'ютера 15 м спостерігається відносна відсутність перешкод, що вносяться різними пристроями. Результати, які характеризують електромагнітну обстановку середовища, представлені на рис. 2.1, 2.2, 2.3.

На рисунках видно, що побічне електромагнітне випромінювання і наведення дисплея займають декілька частотних діапазонів: 30...40 МГц; 50...55 МГц; 110...150 МГц. Побічне випромінювання принтера зафіксовано на частоті 20 МГц. Рівень сигналів має значення від 3...25 дБ при чутливості радіоприймальної системи у 115 дБ/Вт. Дисплей випромінює максимальний рівень сигналу практично з усіх боків окрім екрану.

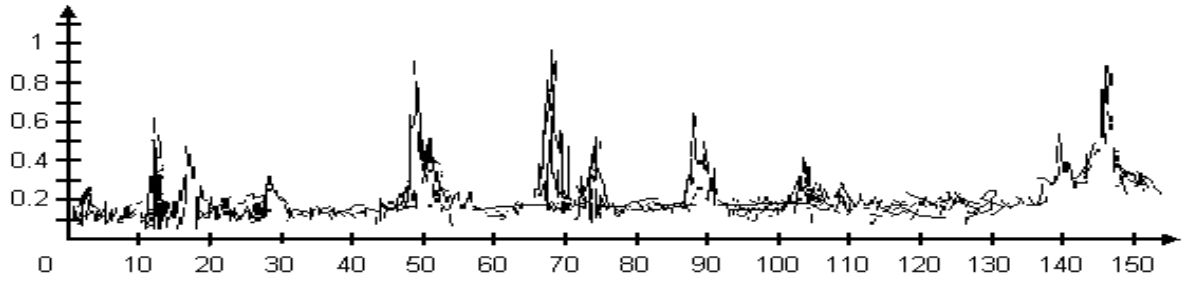


Рис. 2.1. Електромагнітна обстановка при відключеному комп'ютерному обладнанні

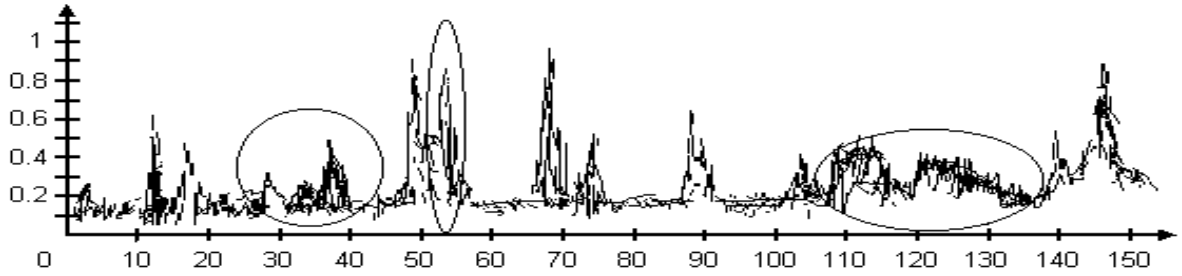


Рис. 2.2. Електромагнітна обстановка при включених моніторі і системному блоці

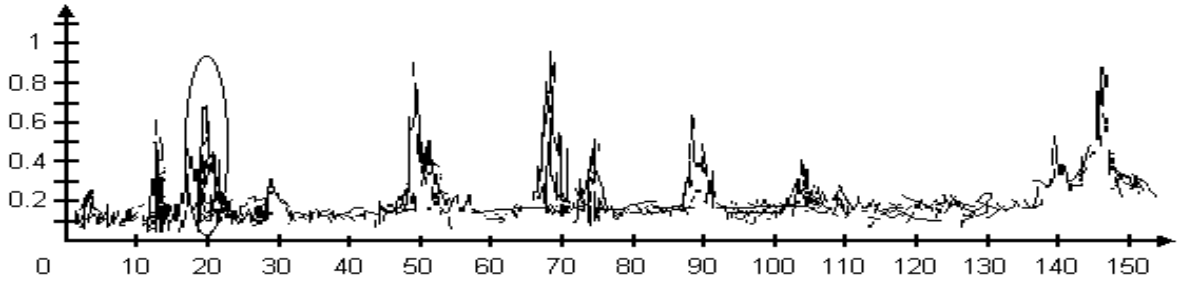


Рис. 2.3. Електромагнітна обстановка при включеному принтері

Екран з розрахунковими характеристиками встановлений по периметру всередині корпусу дисплея показує, що в цьому випадку ПЕМВН можна зафіксувати безпосередньо біля екрану дисплея на відстані 0,2 м.

Тема 3. Методи інформаційної безпеки в комп'ютерних системах і технологіях

3.1. Огляд методів інформаційної безпеки в комп'ютерних системах і технологіях

Як би складна не була техніка приймання, передавання, зберігання і оброблення інформації в комп'ютерних системах і технологіях, до теперішнього часу не втратили своєї актуальності такі традиційні методи як:

- обмеження доступу;
- розмежування доступу;
- розподіл доступу;
- криптографічне перетворення;
- контроль і облік доступу;
- законодавчі заходи.

Зазначені методи реалізуються за допомогою організаційних заходів і технічних засобів. Розширений перелік носіїв інформації, вимагає і складний механізм організації інформаційних процесів. У зв'язку з цим збільшилася кількість випадкових впливів, число каналів витоку інформації від несанкціонованого доступу. Тому одночасно з розвитком інформаційних процесів, поряд з організаційними методами, виникають нові додаткові методи щодо їх захисту в комп'ютерних системах і технологіях, такі як інженерно-технічні та програмно-апаратні.

До організаційних методів слід віднести такі методи як:

- методи функціонального контролю, що забезпечують виявлення і діагностику відмов і збоїв апаратури і помилок людини;
- методи підвищення достовірності прийнятої і оброблюваної інформації;

- методи захисту інформаційних процесів від аварійних ситуацій;
- методи контролю доступу до внутрішнього монтажу апаратури, лініях зв'язку і технологічним органам контролю;
- методи розмежування і контролю доступу до інформації;
- методи ідентифікації і аутентифікації користувачів, технічних засобів, носіїв інформації і документів.

До інженерно-технічних методів інформаційної безпеки відносяться методи:

- пасивного захисту;
- активного захисту.

Програмно-апаратні методи реалізуються з використанням всіх організаційних та інженерно-технічних засобів як на території, де розміщена комп'ютерна система, так і за її межами. Суть програмно-апаратних методів полягає в реалізації обмеження доступу (програмно і/або апаратно) до операційної системи комп'ютера або обчислювальної мережі, програмних засобів оброблення інформації та інформаційних ресурсів.

Всі перераховані методи використовуються і застосовуються в комп'ютерних системах тільки з використанням організаційної складової інформаційної безпеки.

3.2. Організаційні методи інформаційної безпеки в комп'ютерних системах і технологіях

3.2.1. Обмеження доступу

Обмеження доступу полягає у створенні деякої фізичної замкнутої перешкоди навколо об'єкта захисту з організацією контрольованого доступу особи, пов'язаного з об'єктом захисту.

Обмеження доступу до комплексів засобів автоматизації полягає у:

- виділенні спеціальної території для розміщення системи;
- спорудженні по периметру зони спеціальних загороджень з охоронною сигналізацією;
- спорудженні спеціальних будівель або інших споруд;
- виділенні спеціальних приміщень в будівлі;
- створенні контрольно-пропускної системи на територіях, у будинках та приміщеннях.

Завдання засобів обмеження доступу – виключити випадковий і навмисний доступ сторонніх осіб на територію розміщення комп'ютерної системи. У цьому випадку досить добре використовуються традиційні способи (посвідчення особи, контрольно-пропускна система, охоронна сигналізація тощо) і впроваджуються нові досягнення ідентифікації співробітника (відбитки пальців, голосові характеристики тощо).

В наш час підприємства випускають електронні системи для захисту державних і приватних об'єктів від проникнення сторонніх осіб. До таких систем відноситься сигналізація, яка має спеціалізоване автоматизоване підключення до об'єкту охорони через телефонні канали зв'язку.

За принципом дії системи тривожної сигналізації можна класифікувати як:

- традиційні (звичайні), засновані на використанні ланцюгів сигналізації і індикації в комплексі з різними контактами (датчиками);
- ультразвукові;
- телевізійні;
- радіолокаційні;
- мікрохвильові;
- інші.

В наш час на ринку засобів інформаційної безпеки з'являються все нові і нові пристрої, системи та комплекси. Розробляються і приймаються законодавчі акти, які регулюють взаємовідносини власників, користувачів інформаційних ресурсів і служб безпеки.

3.2.2. Контроль доступу до апаратури

З метою контролю доступу до внутрішнього монтажу, лініях зв'язку і технологічним пультів управління використовується апаратура контролю розтину апаратури. Це забезпечується установкою датчиків, які спрацьовують при відкриванні (розбиранні) обладнання, що охороняється. Сигнали з датчиків надходять до автоматизованих систем контролю.

Контроль доступу до внутрішнього монтажу необхідний також для забезпечення технологічної дисципліни обслуговуючого персоналу (з позиції захисту від несанкціонованого доступу) від наступних дій:

- зміни і руйнування принципової схеми комп'ютерної системи;
- підключення стороннього пристрою;
- зміни алгоритму роботи КС шляхом використання технологічних пультів і органів управління;
- завантаження сторонніх програмних продуктів (вірусів тощо);
- використання терміналів сторонніми особами.

Основне завдання контролю відкривання апаратури – перекриття на період експлуатації всіх позаштатних і технологічних підходів. Якщо така ситуація потрібна, то апаратура, що виводиться за межі контуру для ремонту, профілактики тощо, надалі вводиться в контур під наглядом фахівців відповідальних за безпеку інформаційних процесів і захисту інформації.

Доступ до штатних входів в систему – терміналів контролюється за допомогою контролю видачі ключів, а доступ до інформації – за допомогою системи розпізнавання та розмежування доступу, що включає застосування кодів паролів, відповідні функціональні завдання ПЗ та спеціального терміналу служби безпеки інформації. Зазначений термінал і пристрій контролю входить до складу робочого місця служби безпеки інформації.

3.2.3. Розмежування та контроль доступу

Розмежування доступу в комп'ютерній системі полягає в розподілі інформації, що циркулює в ній, на частини і організації доступу до неї посадових осіб відповідно до їх функціональних обов'язків і повноважень.

Завдання розмежування доступу – скорочення кількості посадових осіб, які не мають відношення до комп'ютерної інформаційної системи при виконанні службових обов'язків.

Для забезпечення розмежування і контролю доступу до інформації організація їх обслуговування будується наступним чином:

- технічне обслуговування КС в процесі експлуатації має виконуватися окремим персоналом без доступу до інформації;
- перезавантаження програмного забезпечення і всілякі його зміни повинні проводитися спеціально виділеними для цього фахівцями;
- функції забезпечення безпеки повинні виконуватися спеціальним підрозділом в організації – власника КС, обчислювальної мережі або АСУ;
- організація доступу користувачів до пам'яті КС забезпечувала можливість розмежування доступу до інформації, що зберігає в ній, з достатнім ступенем деталізації і відповідно і відповідно із заданим рівнем повноважень користувачів;
- реєстрація і документування технологічної і оперативної інформації повинні бути розділені.

Розмежування доступу користувачів – споживачів КС може бути:

- за видом, призначенням, ступенем важливості і секретності інформації;
- за способом оброблення: зчитати, записати, внести зміни, виконати команду;
- за умовним номером терміналу;
- за часом оброблення.

На етапі проектування базового комплексу КС реалізують:

- розробку операційної системи з можливістю реалізації розмежування доступу до інформації та інформаційного процесу;
- ізоляцію загального доступу;
- розподіл бази даних на групи;
- процедури контролю перерахованих функцій.

При проектуванні автоматизованих обчислювальних комплексів і баз обробки даних проводиться:

- розробка і реалізація функціональних завдань щодо розмежування і контролю доступу до апаратури та інформації як в межах даної КС, так і в цілому всієї системи;
- розробка апаратних засобів ідентифікації і аутентифікації користувача;
- розробка програмних засобів контролю та управління розмежуванням доступу
- розробка окремої експлуатаційної документації на засоби ідентифікації, аутентифікації, розмежування та контролю доступу.

В якості ідентифікаторів особи для реалізації розмежування широко застосовуються коди паролів, які зберігаються в пам’яті користувача і КС. На допомогу користувачам в системах з підвищеними вимогами великі значення кодів паролів записуються на спеціальні носії – електронні ключі або картки.

3.2.4. Розподіл привілеїв на доступ

Розподіл привілеїв на доступ до інформації полягає в тому, що з числа допущених до нього посадових осіб виділяється група, якій надається доступ тільки при одночасному пред’явленні повноважень всіх членів групи.

Завдання даного методу – істотно ускладнити навмисне перехоплення інформації порушником. Прикладом може служити сейф із замком, який відкривається декількома ключами одночасно. Такий же принцип розподілу привілеїв доступу використовується при використанні в КС.

Цей метод значно ускладнює процедуру роботи, але є високоефективним засобом захисту. На його принципах можна організувати доступ до даних з санкції вищої посадової особи на вимогу або без неї.

Поєднання подвійного криптографічного перетворення інформації і методу розподілу привілеїв дозволяє забезпечити захист інформації від навмисного несанкціонованого доступу.

За наявності дефіциту в коштах, а також з метою постійного контролю доступу до цінної інформації з боку адміністрації і користувача КС в деяких випадках, можливий варіант використання права на доступ до інформації керівника нижчої ланки тільки при наявності його ідентифікатора і ідентифікатора його заступника або представника служби безпеки інформації. При цьому інформація видається тільки на дисплей керівника, а на дисплей підлеглого – тільки інформація про факт її виклику.

3.2.5. Ідентифікація та встановлення автентичності

Об’єкт ідентифікації та встановлення автентичності.

Ідентифікація – це присвоєння будь-якому об’єкту чи суб’єкту унікального образу, імені або числа. Встановлення оригінальності (аутентифікація) полягає в перевірці, чи є об’єкт, що перевіряється (суб’єкт) справді тим за кого себе видає.

Об’єктами ідентифікації можуть бути:

- людина (оператор, користувач);
- технічний засіб (термінал, дисплей, комп’ютер і т. ін.);
- документи (роздруківки, лістінги тощо);
- носії інформації (магнітні диски, флеш-накопичувачі і т. ін.);
- інформація (табло, інформація на дисплеї).

Ідентифікація може бути проведена як спеціальним персоналом, так і технічними засобами.

Ідентифікація та встановлення автентичності особистості. Як ознаки автентичності особистості зовнішні ознаки (зріст, вага, форми окремих частин тіла тощо) правда з часом параметри

людини змінюються, але з розвитком техніки зростає і точність прогнозування цих змін (відбитки пальців, голос тощо). Окрім антропологічних параметрів необхідно уважніше відноситься до конфіденційності, тому що інформація записана на носіях є ключем до інформації, що підлягає захисту. Для цього існує система аутентифікації «ключ-замок». Система «ключ-замок» має локальне застосування. Одним з поширених методів аутентифікації є присвоєння особі або об'єкту унікального імені або числа – пароля і зберігання його в комп'ютерній системі. При вході в комп'ютерну систему користувач відкриває доступ до інформації дозволеної тільки йому.

Алгоритм ідентифікації комп'ютерної системи представлений на рис. 3.1.

Найбільш високий рівень входу в систему є розділення коду на дві частини: одну запам'ятовує користувач і вводить його вручну, друга вводиться за допомогою магнітної чи іншої картки.

На випадок захисту частини пароля від отримання її порушником шляхом фізичного примусу користувача, можливо, буде корисно в обчислювальній системі передбачити механізм тривожної сигналізації, заснованої на застосуванні помилкового пароля. Помилковий пароль запам'ятовується користувачем одночасно з дійсним і повідомляється злочинцеві в екстреній ситуації.

Однак, з огляду на небезпеку для життя користувача необхідно в комп'ютерній системі одночасно з прихованою сигналізацією передбачити механізм обов'язкового виконання вимог злочинця, скориставшись засобами аутентифікації законного користувача.

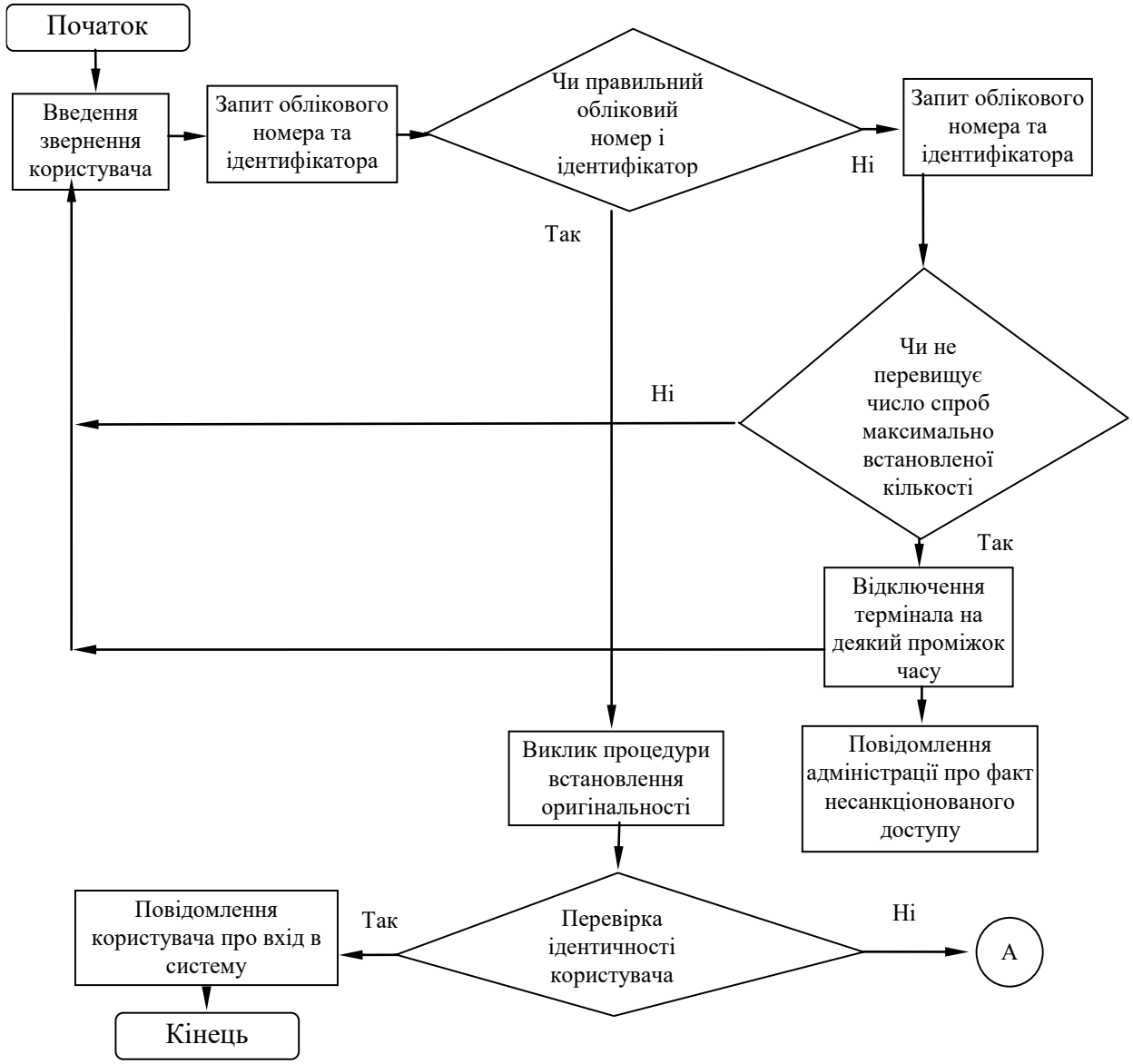


Рис. 3.1. Процедура ідентифікації і встановлення дійсності користувача

Ідентифікація та встановлення автентичності технічних засобів. При організації системи інформаційної безпеки є ідентифікація дійсності технічних засобів. Цей рівень захисту здійснюється за допомогою паролів. Пароль використовується не тільки для користувача і терміналу по відношенню до системи, але і для зворотного встановлення автентичності комп'ютера по відношенню до користувача. Це використовується для роботи з віддаленим об'єктом. У цьому випадку використовуються

одноразові паролі або більш складні системи шифрування інформації.

Ідентифікація та встановлення автентичності документів. У комп'ютерних системах і технологіях документами є роздруківки, лістінги, магнітні носії тощо. Для цього випадку використовується два підходи:

- отримання документа, сформованого безпосередньо в КС і на її документування;
- отримання її з віддалених об'єктів КС.

У першому випадку справжність гарантується системами, що мають засоби захисту від несанкціонованого доступу, а також фізичними характеристиками друкувального пристрою, які властиві тільки для цієї системи. При недостатності цих заходів необхідно використовувати криптографічне перетворення. Це особливо актуально для другого випадку, коли документ доставляється без охорони з території віддаленого об'єкта. При цьому до носія додаються документи з підписами відповідальних осіб, завіреними печатками.

При неавтоматизованому обміні інформацією справжність документів засвідчується особистим підписом людини, автора документа. Перевірка здійснюється візуально за особистими документами.

При автоматизованій передачі документів по каналах зв'язку, розташованим на неконтрольованій території, змінюються умови обміну. Так як в цьому випадку підробка підпису документів є відносно простою, то використовується так званий електронний підпис. Цим користуються організації, що займаються банківською та іншою життєво важливою діяльністю. При цьому учасники потребують захисту від навмисних НСД у вигляді:

- відмови відправника від переданого повідомлення;
- зміни одержувачем отриманого повідомлення;
- маскування відправника під інше повідомлення;

Забезпечення захисту кожної сторони, що бере участь в обміні інформацією, здійснюється за допомогою ведення спеціальних протоколів. Для верифікації використовують такі положення:

- відправник вносить в передану інформацію свій електронний підпис, що представляє собою додаткову інформацію, яка включає ім'я одержувача і деяку закриту інформацію, якою володіє тільки відправник;
- одержувач повинен мати можливість упевнитися в тому, що в складі повідомлення підпис є справжнім підписом відправника;
- отримання правильного підпису відправника можливо тільки при використанні закритої інформації, якою володіє тільки відправник;
- для виключення можливості повторного використання застарілого повідомлення верифікація повинна залежати від часу.

Підпис повідомлення являє собою спосіб шифрування повідомлення з допомогою криптографічного перетворення. Закриваючим елементом в перетворенні є код ключа.

Ідентифікація та встановлення автентичності інформації на засобах її відображення і друку. У комп'ютерних системах і технологіях з централізованою обробкою даних і відносно низькими вимогами до захисту встановлення її справжності на технічних засобах відображення інформації гарантується даної КС. Однак з ускладненням системи збільшується і ймовірність виникнення несанкціонованого доступу до інформації, її модифікації та розкрадання. Тому в більш відповідальних випадках окремі повідомлення або блоки інформації піддаються спеціальному захисту, який полягає у створенні засобів підвищення достовірності інформації, її криптографічного перетворення. Встановлення дійсності отриманої інформації, включаючи відображення на табло і терміналах, полягає в контролі забезпечення достовірності інформації, результатів дешифрування отриманої інформації до відображення її на дисплеї. Справжність інформації на засобах її відображення тісно пов'язана з достовірністю документів. Тому всі положення приведені раніше

справедливі і для цього випадку. Чим ближче до поля відображення (паперового носія) ця процедура наближається, тим вірогідніше відображається інформація.

3.3. Інженерно-технічні методи інформаційної безпеки

Організації, що експлуатують персональні комп'ютери або автоматизовані комплекси, що базуються на мікропроцесорній техніці, зіштовхуються з проблемами інформаційної безпеки, яка обробляється та зберігається в КС. При створенні і експлуатації систем безпеки необхідно враховувати виконання ряду умов:

- заборона на доступ до інформаційних ресурсів без створення необхідних для цього умов;
- простота механізму захисту;
- закриття всіх можливих каналів витоку.

Практично всі програмно-апаратні ЗЗІ від несанкціонованого доступу в тій чи іншій мірі передбачають виконання перших двох умов. Однак при проектуванні не завжди враховується можливість «злому» системи шляхом аналізу електромагнітних наведень і випромінювань, що проходять між засобом ідентифікації користувача і апаратною частиною ЗЗІ, яка встановлюється в комп'ютері чи у мікропроцесорному блоці обробки сигналів. Це створює передумови відновлення протоколів обміну між ідентифікаторами та апаратною частиною ЗЗІ по радіоканалу. Причому величина зони випромінювання, на якій може бути перехоплення радіосигналів, що містять інформацію про протокол обміну, може досягати десятка метрів. Зокрема, цей недолік є у засобів захисту і систем контролю доступу в приміщення, реалізованих на основі електронних ідентифікаторів сімейства DS 199x. Природно, що виявити в цьому випадку пристрої знімання інформації досить проблематично. Тим більше що, незважаючи на

укази Президента і закони в галузі інформаційної безпеки, на українському ринку найчастіше пропонуються різні системи перехоплення і аналізу побічних електромагнітних випромінювань і наведень (ПЕМВН).

Інженерно-технічний захист інформації – одна з основних складових комплексу заходів щодо інформаційної безпеки, яка становить державну та комерційну таємницю. Проблеми інформаційної безпеки поглиблюються ще й недосконалістю законодавчої бази щодо збереження державної та комерційної таємниць.

Інженерно-технічний захист інформації включає комплекс організаційних і технічних заходів щодо забезпечення інформаційної безпеки, на основі організаційних заходів технічними засобами і вирішує наступні завдання:

1. Запобігання проникнення зловмисника до джерел інформації з метою її знищення, розкрадання або зміни.

2. Захист носіїв інформації від знищення в результаті впливу стихійних сил і, перш за все, пожежі і води (піни) при її гасінні.

3. Запобігання витоку інформації з різних технічних каналів.

Способи і засоби вирішення перших двох завдань не відрізняються від способів і засобів захисту будь-яких матеріальних цінностей, третє завдання вирішується виключно способами і засобами інженерно-технічного захисту інформації.

Інженерно-технічний захист інформації являє собою галузь науки і техніки, що розвивається на стику теорії систем, фізики, оптики, акустики, радіоелектроніки, радіотехніки, електро- і радіовимірювань та інших дисциплін. Коло питань, якими змушений займатися інженерно-технічний захист, широкий і обумовлений різноманіттям джерел та носіїв інформації, способів і засобів її здобування, а, отже, і захисту. Для забезпечення ефективного інженерно-технічного захисту інформації необхідно визначити:

- що захищати технічними засобами в даній організації, будівлі, приміщенні;

- які загрози має інформація з боку зловмисників і їх технічних засобів, які способи і засоби доцільно застосовувати для забезпечення інформаційної безпеки з урахуванням як величини загрози, так і витрат на її запобігання;
- як організувати і реалізувати технічний захист інформації в організації.

Без цих знань захист інформації може проводитися у формі кругової оборони (при необмежених ресурсах) або «латання дірок» в більш реальному варіанті обмеженості коштів.

При організації інформаційної безпеки, як і інших видів захисту, необхідно також знати і враховувати психологічні чинники, що впливають на прийняття рішення керівником або будь-якою іншою відповідальною особою. Це обумовлено тим, що заходи із захисту мають превентивну спрямованість без достатньо достовірних даних про потенційні загрози не взагалі, а стосовно конкретної організації. Крім того, наслідки прихованого розкрадання інформації проявляються через деякий час, коли часом буває досить важко виявити справжню причину погіршення фінансового становища фірми або появи у конкурента ідентичної продукції. Ці фактори не сприяють психологічній готовності керівника на досить великі витрати на захист інформації. Проте, світовий досвід організації захисту інформації підтверджує, що на інформаційну безпеку фірми змушені виділяти близько 10-20% від загального прибутку. Оскільки значну частину витрат на захист інформації складають витрати на придбання і експлуатацію засобів захисту, то методологія інженерно-технічного захисту інформації повинна забезпечувати можливість раціонального вибору засобів інформаційної безпеки. Тому основи інженерно-технічного захисту інформації повинні містити як теоретичні знання, так і методичні рекомендації, що забезпечують вирішення цих завдань. Серед методів інженерно-технічного захисту слід виділити: пасивні, активні і комбіновані методи.

3.3.1. Пасивні методи інженерно-технічного захисту

Пасивні методи захисту інформації спрямовані на:

- ослаблення побічних електромагнітних випромінювань (інформаційних сигналів) технічних засобів передавання інформації на межі контрольованої зони;
- ослаблення наведень побічних електромагнітних випромінювань і наведень технічними засобами передавання інформації;
- виключення (ослаблення) просочування інформаційних сигналів у колі електроживлення, що виходять за межі комп'ютерних систем.

3.3.2. Активні методи інженерно-технічного захисту

Активні методи захисту інформації спрямовані на:

- створення маскувальних просторових електромагнітних завад з метою зменшення відношення сигнал/шум на межі контрольованої комп'ютерної системи;
- створення маскувальних електромагнітних перешкод в сторонніх провідниках і сполучних лініях телекомунікаційних та силових ланцюгах з метою зменшення відношення сигнал/шум на межі контрольованої комп'ютерної системи.

3.4. Програмно-апаратні методи захисту інформації

Програмно-апаратні методи інформаційної безпеки засновані на основі використання засобів, що містять в своєму складі елементи, які реалізують функції захисту інформації, в яких програмні (мікропрограмні) і апаратні частини повністю взаємозалежні і неподільні.

На початковому етапі розвитку методів і засобів інформаційної безпеки захист здійснювався на програмному рівні, наприклад перевірка цілісності програмного середовища іншою, спеціально розробленою програмою. Але, зважаючи на те, що спеціальна програма перебувала на одному носії з об'єктами перевірки, такі методи не можуть дати гарантії правильності проведення процедур. При цьому необхідно проводити перевірку самої перевіряючої програми. Таким чином, необхідно використання апаратних засобів із вбудованими процедурами контролю цілісності програм і даних, ідентифікації і аутентифікації, реєстрації та обліку.

Об'єктом програмно-апаратного захисту є:

- персональний комп'ютер;
- інформаційні ресурси;
- мережеві (телекомунікаційні) засоби:
- інформаційні технології.

Для забезпечення заданого рівня захисту інформаційних процесів та інформації необхідно використовувати такі методи програмно-апаратного захисту як:

- аутентифікації учасників інформаційної взаємодії;
- захисту технічних засобів від несанкціонованого доступу;
- розмежування доступу до документів, ресурсів персонального комп'ютера і мережі;
- захисту електронних документів;
- захисту даних в каналах зв'язку;
- захисту інформаційних технологій;
- розмежування доступу до вхідних потоків даних.

Учасниками інформаційними взаємодії є оператори і віддалені користувачі. Аутентифікація/ідентифікація операторів виконується апаратно до етапу завантаження операційної системи. Бази даних ідентифікації/аутентифікації повинні зберігається в незалежній пам'яті системи інформаційної безпеки, організованої так, щоб доступ до неї засобами персонального комп'ютера був неможливий, тобто незалежна пам'ять повинна бути розміщена

поза адресним простором комп'ютера. Програмне забезпечення контролера має зберігатися в пам'яті спеціального контролера, захищеного від несанкціонованих модифікацій. Цілісність програмного забезпечення забезпечується технологією виготовлення контролера системи захисту. Ідентифікація здійснюється із застосуванням відчужуваного носія інформації.

Аутентифікація/ідентифікація віддалених користувачів виконується з використанням апаратної реалізації. Процедура аутентифікації може бути виконана різними способами, включаючи електронний цифровий підпис. Обов'язковою є вимога «посиленої аутентифікації», тобто періодичного повторення процедури в процесі роботи через інтервали часу, досить малі для того, щоб при подоланні захисту порушник не міг нанести відчутного збитку.

Захист технічних засобів від несанкціонованого доступу забезпечуються електронними замками і апаратними модулями довіреного завантаження. Різниця способів захисту полягає в реалізації контролю цілісності. Електронні замки апаратно виконують процедури ідентифікації/аутентифікації з використанням зовнішнього програмного забезпечення для виконання процедура перевірки контролю цілісності. Апаратні модулі довіреного завантаження реалізують як функції електронних замків, так і функції контролю цілісності і функції адміністрування. В результаті забезпечується не тільки функції ідентифікації/аутентифікації користувача, але і здійснюється довірене завантаження операційної системи – найважливіша функція для побудови ізольованого програмного середовища. Функціонально апаратні модулі довіреного завантаження значно повніші, ніж електронні замки. Модулі вимагають апаратної (без використання ресурсів операційної системи) реалізації складних функцій, таких, як розбір файлових систем (ФС), забезпечення читання реальних даних та ін. При цьому, за рахунок інтеграції контрольних функцій в апаратурі, модулі довіреного завантаження забезпечують також більш високу надійність і достовірність результатів.

Контроль цілісності технічного складу комп'ютера повинен виконуватися контролером ЗЗІ до завантаження ОС. При цьому повинні контролюватися всі ресурси, які (потенційно) можуть використовуватися спільно, в тому числі:

- центральний процесор;
- системний BIOS;
- додатковий BIOS;
- вектори переривань;
- CMOS, зокрема оптичних дисків, флеш носіїв, жорстких дисків тощо.

Цілісність технічного складу ЛОМ забезпечується процедурою посиленої аутентифікації мережі. Процедура повинна виконуватися на етапі підключення перевіреного комп'ютера до мережі і далі через заздалегідь визначені адміністратором безпеки інтервали часу.

Посилена аутентифікація повинна виконуватися із застосуванням рекомендованого варіанту апаратного датчика випадкових чисел. Якість роботи датчика має контролюватися системою рекомендованих тестів.

Контроль цілісності системних областей і файлів ОС повинен виконуватися контролером до завантаження ОС, чим забезпечується механізм читання реальних даних. Так як в електронному документообігу можуть використовуватися різні операційні системи, то вбудоване в контролер програмне забезпечення має забезпечувати розбір найбільш популярних файлових систем.

Цілісність даного програмного забезпечення повинна гарантуватися технологією виготовлення контролерів з системою захисту інформації.

Захист програмного забезпечення від несанкціонованих модифікацій повинен забезпечуватися апаратними засобами контролера.

Для контролю цілісності повинна застосовуватися відома (опублікована) хеш-функція, еталонне значення якої повинно

зберігатися в незалежній пам'яті контролера, захищеної апаратно від доступу з комп'ютера.

Контроль цілісності програмного забезпечення та даних може виконуватися як апаратною компонентою, так і програмною компонентою системи захисту в тому випадку, якщо її цілісність була зафіксована апаратно на попередньому етапі. Для контролю цілісності повинна застосовуватися відома (опублікована) хеш-функція, еталонне значення якої повинно аутентифікуваться за допомогою відчужуваного технічного носія інформації (ідентифікатора).

Розмежування доступу до документів, ресурсів комп'ютера і мережі. Сучасні операційні системи (ОС) містять вбудовані засоби розмежування доступу. Ці засоби використовують особливості конкретної файлової системи і засновані на атрибутах, пов'язаних з одним з рівнів інтерфейсу API операційної системи.

Прив'язка до особливостей файлової системи. В сучасних операційних системах, як правило, використовуються не одна, а кілька ФС – як нові, так і застарілі. При цьому зазвичай на новій ФС вбудоване в ОС розмежування доступу працює, а на старій – може і не працювати, так як використовує суттєві відмінності нової ФС. Ця обставина зазвичай прямо не зазначається в сертифікаті, що може ввести користувача в оману. Уявімо, що на комп'ютері з новою ОС експлуатується програмне забезпечення, розроблене для попередньої версії, орієнтоване на особливості колишньої ФС. Користувач має право вважати, що встановлені захисні механізми, сертифіковані і призначені саме для використовуваної ОС, будуть виконувати свої функції, тоді як в дійсності вони будуть відключені. У реальному житті з метою забезпечення сумісності старі ФС і включаються до складу нових ОС.

Прив'язка до API операційної системи. Як правило, операційні системи змінюються зараз дуже швидко – 1-2 рази на рік. Не виключено, що будуть змінюватися ще частіше. Деякі такі зміни пов'язані зі змінами, в тому числі і API. Якщо при цьому атрибути розмежування доступу відображають склад API – з переходом на сучасну версію ОС буде необхідно переробляти

налаштування системи безпеки, проводити перенавчання персоналу тощо.

Таким чином, можна сформулювати загальну вимогу – підсистема розмежування доступу повинна бути накладеною на операційну систему, і тим самим, бути незалежною від файлової системи. Зрозуміло, склад атрибутів повинен бути достатній для цілей опису політики безпеки, причому опис має здійснюватися не в термінах API ОС, а в термінах, в яких звично працювати адміністраторам безпеки.

Захист електронних документів. Життєвий цикл електронного документа протікає в трьох середовищах існування, вкладених одне в інше:

- електронне – середовище цифрових процесів;
- аналогове – середовище об’єктів, предметів;
- соціальне – середовище мислячих суб’єктів.

Зовнішня оболонка – підмножина мислячих суб’єктів соціального середовища, утворює сектор дієвості документа, який диктує правила обміну інформацією свої членам-суб’єктам, в тому числі, вимоги до технології взаємодії. Якщо ці правила і вимоги виконані, то повідомлення визнається документом, а інформація, що міститься в ньому, визнається сектором як (юридичний) факт – формальною підставою для виникнення, зміни, припинення конкретних відносин між суб’єктами суспільства.

Вимоги сектора дієвості можна розділити на семантичні, що пред’являються до відображення сенсу інформації, і технологічні, які диктують правила оформлення документа. Семантичні аспекти є прерогативою соціального середовища, і тому тут не розглядаються і вважаються виконаними. За такої умови для визнання повідомлення документом необхідно, щоб параметри технологій, використаних при його формуванні, перетворенні, передаванні та зберіганні, лежали б у межах допустимих відхилень від деякого еталона, який пропонується сектором для документального електронної взаємодії. Тільки в цьому випадку виникають юридичні підстави вважати, що виконуються вимоги,

наприклад, щодо забезпечення цілісності, конфіденційності, автентичності документа.

Традиційний, аналоговий документ (АнД) формується одноразово у вигляді предмета – аркуша паперу з поверхнею, розфарбованою візерунками-літерами. Фізичні параметри предмета стійкі до зовнішнього впливу, їх зміна порівняно просто відображається, протягом всього життєвого циклу предмет-документ не перетвориться в інший предмет, в будь-який момент часу АнД зосереджений в єдиній точці простору, так що можливості несанкціонованого доступу обмежені. Вибір можливих традиційних інформаційних технологій вузький, так що вимоги еталонної технології очевидні за замовчуванням.

Інша річ – електронний документ (ЕлД). Легкість і простота модифікації ЕлД закладена самим середовищем його існування: операції копіювання і заміни є фундаментальними в машині Тьюрінга. ЕлД багаторазово перетворюється протягом життєвого циклу, фізична індикація спотворення ЕлД важка. Вимоги відповідності застосовуваних інформаційних технологій еталонним технологіям вкрай значимі. Тому захист електронного обміну інформацією включає два класи завдань: забезпечення еквівалентності документа протягом його життєвого циклу вихідного ЕлД – еталону; забезпечення еквівалентності застосованих електронних технологій еталонним, що встановлені сектором дієвості.

В електронному середовищі не має сенсу інтерпретація інформації як відомостей, сенсу, знання, факту. Для комп’ютера вірші і випадкове число – це множини двійкових біт, на якому поставлено порядок – послідовність нульових і одиничних біт. Будь-які дві множини відображають одну і ту ж інформацію, якщо зберігається задане відношення впорядкованості – якщо множини ізоморфні. Так як двійкову обмежену послідовність завжди можна перетворити в число, то в електронному середовищі інформація є число. Число не змінюється в часі і просторі, воно завжди фіксоване, статичне. При зберіганні на диску пам’яті число відображається «розфарбуванням» поверхні диска магнітними

доменами з різною орієнтацією. Тобто, в пам'яті ЕОМ зберігаються дані, які розуміються як фіксована форма існування електронної інформації: дані – це число.

Призначення будь-якого захисту – забезпечення стабільності (фіксованості!) заданих властивостей об'єкта, що захищається в усіх точках життєвого циклу. Захищеність об'єкта відображається зіставленням еталона (об'єкта у вихідній точці простору і часу) і результату (об'єкта в момент спостереження). У нашому випадку в точці спостереження (отримання ЕлД) є тільки дуже обмежена контекстна інформація про ідеал (зміст вихідного ЕлД), проте є повна інформація про результат (що спостерігається в документі). Це означає, що ЕлД повинен включати в свій склад атрибути, що засвідчують дотримання технічних і технологічних вимог, тобто незмінність повідомлення на всіх етапах виготовлення і транспортування документа. Одним з варіантів атрибутів можуть бути захисні коди аутентифікації (ЗКА).

Захист документа при його створенні. При створенні документа повинен апаратно вироблятися захисний код аутентифікації (ЗКА). При цьому до початку формування ЗКА повинна бути забезпечена ізольованість програмного середовища (ІПС). Запис копії електронного документа на зовнішні носії до формування ЗКА повинна бути виключена. Якщо ЕлД породжується оператором, то ЗКА повинен вироблятися з прив'язкою до оператора. Якщо ЕлД породжується програмною компонентою АС, то ЗКА повинен вироблятися з прив'язкою до даної програмної компоненти.

Захист документа при його передаванні по зовнішнім (відкритим) каналам зв'язку повинна виконуватися на основі застосування сертифікованих криптографічних засобів, у тому числі з використанням електронно-цифрового підпису (ЕЦП) для кожного переданого документа. Можливий і інший варіант – за допомогою ЕЦП підписується пачка документів, а кожен окремий документ засвідчується іншим аналогом власноручного підпису (АВП) – наприклад, ЗКА.

Захист документа при його обробці, зберіганні та використанні. На цих етапах захист документа здійснюється застосуванням двох ЗКА – вхідного і вихідного для кожного етапу. При цьому ЗКА повинні вироблятися апаратно з прив'язкою ЗКА до процедури обробки (етапу інформаційної технології). Для надходження документа (з ЗКА і ЕЦП) здійснюється $ЗКА_2$ і тільки потім знімається ЕЦП. Потім на наступному етапі (n) здійснюється $ЗКА_{n+1}$ і знімається $ЗКА_{n-1}$. Таким чином, в будь-який момент часу документ захищений двома ЗКА – $ЗКА_n$ і $ЗКА_{n+1}$. ЗКА повинні вироблятися і перевірятися для документа, розміщеного в оперативній пам'яті ЕОМ, у якій створена і підтримується ІПС. Зняття $ЗКА_{n-1}$ виконується після установки $ЗКА_{n+1}$.

Захист документа при доступі до нього з зовнішнього середовища включає два вже описаних механізму – ідентифікація/аутентифікація віддалених користувачів і розмежування доступу до документів, ресурсів комп'ютера і мережі.

Захист даних в каналах зв'язку. Традиційно для захисту даних в каналі зв'язку застосовують канальні шифратори, і альтернативи цьому немає. Потрібно пам'ятати про дві речі – про сертифікацію, та про те, що по каналах передаються не тільки дані, але і управляючі сигнали.

Захист інформаційних технологій. Електронні документи в АС не тільки зберігаються, а й обробляються. Комп'ютер – це не тільки пам'ять, а й обчислення. При обробці документа одні дані зникають, інші виникають, хоча інформація залишається тією ж самою. Числа змінюються, а інформація – ні, так як зберігається ізоморфізм між множинами двійкових сигналів при «старому» і «новому» форматах. В електронному середовищі принципово повинна існувати якась нова форма існування інформації, відповідна процесу перетворення даних – інформація не може зникнути між «входом» і «виходом» процесу. Але процес динамічний, що є зміною чогось у часі, тоді як інформація повинна бути постійною. Щоб уникнути протиріччя, необхідно, щоб динамічний процес мав якусь фіксовану в часі, статичну,

характеристику – фіксованість опису процесу в часі, в якій би точці простору (комп'ютері) і момент часу цей процес не спостерігався.

Дійсно, конкретний процес обробки інформації в ЕОМ визначається фіксованим алгоритмом, процедурою, протоколом. Припустивши, що в електронному середовищі існують дві форми відображення інформації: статична – у формі об'єкта, динамічна – в формі процесу, ми тим самим припустили два кардинально відмінних класи елементів електронного середовища. Якщо перший клас визначений як числа, то другий, як функції (перетворення, відображення). На «вхід» функції надходять числа-дані, на «виході» з'являються нові числа-дані. У будь-який момент часу і в будь-якій точці простору функція залишається функцією. Функція (або споріднені поняття – відображення, алгоритм, перетворення), – незмінні.

В пасивній формі (зберігання) ЕлД є фіксованим об'єктом в аналоговому середовищі (пристрій пам'яті), в активізованій формі ЕлД існує як фіксований процес в електронному середовищі. Відповідно, виділимо дві складових захисту: захист даних (чисел) – власне ЕлД як фізичного об'єкта; захист процесів (функцій), які реалізують активізовану форму існування ЕлД. Інформація-дані визначається як множина із заданим на ньому відношенням порядку. Захист функцій, тобто алгоритмів, означає захист обчислювального середовища, інваріантного до тієї інформації, тих даних, які в ній обробляються. Електронна технологія також є впорядкована множина (операцій, процесів), і тому формально може бути визнана як інформація-технологія. Вищенаведене виявляє внутрішню єдність складових захисту – це захист інформації-даних і захист інформації-технології.

Таким чином, статус документа передбачає не тільки ідентичність (відповідність стандарту) власне документа, але і відповідність еталонним вимогам застосованих інфотехнологій.

Незважаючи на схожість, механізми захисту власне ЕлД як об'єкта (число, дані) і захист ЕлД як процесу (функція, обчислювальне середовище) радикально відрізняються. При захисті інформації-технології, на відміну від захисту ЕлД, достовірно

відомі характеристики необхідної технології – еталона, але є обмежені відомості про виконання цих вимог фактично використаної технологією – про результат. Єдиним об'єктом, який може нести інформацію про фактичну технологію (як послідовність операцій), є власне ЕлД, а точніше – атрибути, що входять до нього. Як і раніше, одним з видів цих атрибутів можуть бути ЗКА. Еквівалентність технологій може бути встановлена тим точніше, чим більша кількість функціональних операцій прив'язується до повідомлення через ЗКА. Механізми при цьому не відрізняються від застосовуваних при захисті ЕлД. Більш того – можна вважати, що наявність конкретного ЗКА характеризує наявність в технологічному процесі відповідної операції, а значення ЗКА – характеризує цілісність повідомлення на даному етапі технологічного процесу.

Розмежування доступу до потоків даних. Для цілей розмежування доступу до потоків даних використовуються, як правило, маршрутизатори з функцією «VPN». Надійно ця функція може бути реалізована тільки за допомогою криптографічних засобів, де особлива увага повинна приділятися ключовій системі і надійності зберігання ключів. Природно, що вимоги до політики доступу при розмежуванні потоків абсолютно відрізняються від таких при розмежуванні доступу до файлів і каталогів. Тут можливий тільки найпростіший механізм – доступ дозволений або заборонений.

Виконання перерахованих вимог забезпечує достатній рівень захищеності ЕлД як виду повідомлень, що оброблюються в інфосистемах.

Тема 4. Аналіз і оцінювання міцності інформаційної безпеки у комп'ютерних системах і технологіях

4.1. Основи теорії інформаційної безпеки від несанкціонованого доступу

4.1.1. Модель поведінки потенційного порушника

Порушенням вважається спроба несанкціонованого доступу до інформаційних процесів, що захищаються. Оскільки неможливо передбачити час і місце НСД, то, у загальному випадку, доцільно створити модель поведінки потенційного порушника, передбачаючи найбільш небезпечну подію у наступних ситуаціях:

1) порушник може з'явитися в будь-який час в периметрі зони, що охороняється;

2) кваліфікація і обізнаність порушника може бути на рівні розробника даної КС;

3) інформація, що постійно зберігається і принципи роботи системи (включаючи секретну інформацію) порушнику відома;

4) для досягнення своєї мети порушник вибере найбільш слабку ланку в захисті;

5) порушником може бути не тільки стороння особа, а й законний користувач;

6) порушник діє один.

На основі аналізу переліку небезпечних ситуацій для вибору моделі поведінки потенційного порушника доцільно застосування диференційованого підходу. Оскільки кваліфікація порушника поняття відносне, то у загальному випадку, за основу приймається чотири класи безпеки:

1-й клас рекомендується для захисту життєво важливої інформації, витік, руйнування або модифікація якої може привести до катастрофічних наслідків. Міцність захисту повинна бути розрахована на порушника-професіонала;

2-й клас рекомендується використовувати для захисту важливої інформації при роботі декількох користувачів, що мають доступ до різних масивів даних або формують свої файли, недоступні іншим користувачам. Міцність захисту повинна бути розрахована на порушника високої кваліфікації, але не зломщика-професіонала;

3-й клас рекомендується використовувати для захисту щодо важливої інформації, постійний несанкціонований доступ до якої шляхом її накопичення може призвести до витоку більш важливої інформації. Міцність захисту при цьому повинна бути розрахована на відносно кваліфікованого порушника-професіонала;

4-й клас рекомендується для захисту іншої інформації, що не представляє інтересу для серйозних порушників. Однак його необхідність диктується дотриманням технологічної дисципліни обліку та обробки інформації службового користування з метою захисту від випадкових порушень в результаті безвідповідальних користувачів і деякої підстраховки від випадків навмисного несанкціонованого доступу.

Реалізація перерахованих рівнів безпеки повинна забезпечуватися необхідним набором засобів захисту відповідно до очікуваного класу потенційного порушника. Рівень безпеки захисту всередині класу забезпечується кількісною оцінкою міцності окремих засобів захисту і оцінкою міцності контуру захисту від навмисного НСД за розрахунковими формулами.

4.1.2. Модель захисту інформаційного процесу

Модель елементарного захисту. Модель елементарного захисту інформації представлено на рис. 4.1, де предмет захисту поміщений у замкнуту захисну оболонку, яку називають

перешкодою. Міцність захисту залежить від властивостей перешкоди. Здатність протистояти вторгненню з боку порушника характеризується міцністю перешкоди. Таким чином проводиться оцінювання захищеності інформації та їх процесів КС.

Міцність створеної перешкоди вважається достатньою, якщо вартість очікуваних витрат на її подолання потенційним порушником перевищує вартість, інформації, що захищається. Однак можливий і інший підхід оцінювання міцності захисту.

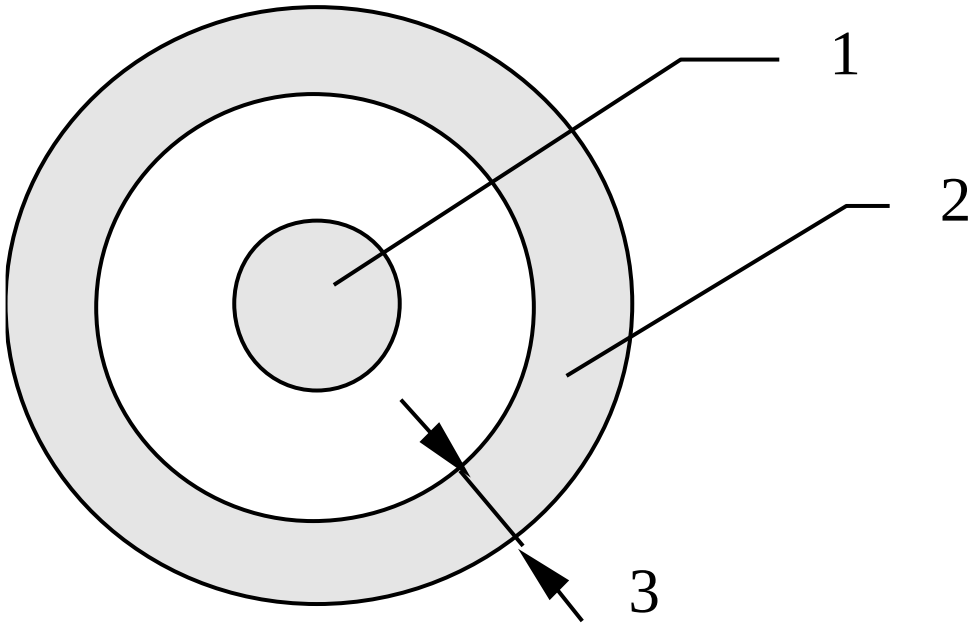


Рис. 4.1. Модель елементарного захисту
(1 – предмет захисту; 2 – перешкода; 3 – міцність перешкоди)

Відомо, що інформація з часом втрачає свою привабливість, старіє, а в окремих випадках, її ціна може впасти до нуля. Тоді за умови достатності захисту можна прийняти перевищення витрат часу на подолання перешкоди порушником над часом життя інформації. Якщо ймовірність неподолання перешкоди порушником через $P_{ЗЗІ}$, час життя інформації через $t_ж$, очікуваний час подолання перешкоди порушником через $t_п$, ймовірність обходу перешкоди порушником через $P_{обх}$, то для випадку старіння інформації умова достатності представляється у вигляді:

$Р_{ЗЗІ} = 1$, якщо $t_ж < t_п$ і $Р_{обх} = 0$.

$Р_{обх}$ рівне нулю, відображає необхідність замикання перешкоди навколо предмета захисту. Якщо $t_ж > t_п$, а $Р_{обх} = 0$, то

$$Р_{ЗЗІ} = (1 – Р_{пр}), \qquad (4.1)$$

де $Р_{пр}$ – ймовірність подолання перешкоди порушником за час менший $t_ж$.

Для реального випадку, коли $t_ж > t_п$ і $Р_{обх} > 0$, міцність захисту представляється у вигляді:

$$Р_{ЗЗІ} = (1 – Р_{пр}) (1\ Р_{обх}),$$

$Р_{пр} = 0$, якщо $t_ж < t_п$; $Р_{пр} > 0$, якщо $t_ж \geq t_п$.

Останній вираз справедливий при наявності двох порушників, тобто коли один долає перешкоду, інший в цей час її обходить. За умови, якщо в наявності є один порушник, то він вибере найбільш простий варіант, тобто:

$$Р_{ЗЗІ} = (1\ Р_{пр}) \cup (1\ Р_{обх}), \qquad (4.2)$$

де знак $\cup$ означає логічну дію «АБО»

Отже, міцність перешкоди після визначення і порівняння буде дорівнювати меншому значенню з них (4.2).

Як приклад елементарного захисту, що розраховується за формулою (4.2), можна назвати криптографічний захист інформації, де величина $Р_{пр}$ може бути визначена шляхом оцінювання ймовірності підбору коду ключа, за допомогою якого можна дешифрувати закриту інформацію, що визначається за формулою:

$$P_{пр} = \frac{n}{A^S}, \qquad (4.3)$$

де n – кількість спроб підбору коду;

A – число символів в обраному алфавіті коду ключа;

S – довжина коду ключа в кількості символів.

Величина $P_{обх}$ – залежить від обраного методу шифрування, способу застосування, повноти перекриття тексту інформації, існуючих методів криптоаналізу, а також способу зберігання дійсного значення коду ключа і періодичності його заміни на нове значення, якщо інформація, закрита даним способом, постійно зберігається у власника. Можливі також і інші обставини, що впливають на ймовірність обходу криптографічного захисту. Вибір і визначення конкретної величини $P_{обх}$ спочатку проводиться експертним шляхом на основі досвіду фахівця. Величина $P_{обх} = 1$ захисту втрачає будь-який сенс.

Можлива також і інша ситуація при якій у однієї перешкоди є кілька шляхів обходу. Тоді вираз (4.2) набуде вигляду:

$$P_{ЗЗІ} = (1\ P_{пр}) \cup (1\ P_{обх1}) \cup (1\ P_{обх2}) \cup ... \cup (1\ P_{обхk}), \qquad (4.4)$$

де k – число шляхів обходу перешкоди, тобто міцність перешкоди дорівнює найменшому значенню, отриманому після визначення і порівняння величин

$$(1 - P_{пр}), (1\ P_{обх1}), (1\ P_{обх2}), ..., (1\ P_{обхk}).$$

У разі якщо інформація, що підлягає захисту, не старіє або періодично оновлюється, тобто $t_ж > t_п$ постійно або коли $t_п > t_ж$ неможливо забезпечити, то застосовується постійно діюча перешкода, що володіє властивостями виявлення і блокування доступу порушника до предмету або об'єкту захисту. Як захист використовується людина або автоматизована система під контролем людини. Безумовно, параметри цієї перешкоди будуть впливати на її міцність.

Здатність перешкоди виявляти і блокувати НСД повинна враховуватися при оцінці її міцності шляхом введення в розрахункову формулу (4.4) замість $(1\ P_{пр})$, де $P_{вбл}$ – ймовірність виявлення і блокування несанкціонованого доступу.

Принцип роботи автоматизованої перешкоди заснований на тому, що здійснюється періодичний контроль датчиків виявлення порушника. Періодичність контролю може досягати сотих часток секунди і менше. У цьому випадку очікуваний час подолання

перешкоди порушником перевищує час опитування датчиків виявлення. Тому такий контроль вважається постійним. Але для виявлення порушника людиною (оператором) цього недостатньо. Потрібен час для спрацьовування тривожної сигналізації, так це час значно перевищує час опитування датчиків і тим самим збільшується час виявлення порушника. Практика показує, що сигнал тривоги, як правило, зупиняє дії порушника, якщо цей сигнал дійшов до нього. Але оскільки фізичний доступ до об'єкту ще відкритий, то охорона повинна локалізувати порушника і організувати його блокування.

Таким чином, умова міцності перешкоди з виявленням і блокуванням НСД можна представити у вигляді співвідношення:

$$\frac{T_{Д} + t_{спр} + t_{вм} + t_{бл}}{t_{Н}} < 1, \qquad (4.5)$$

де $T_д$ – період опитування датчиків;

$t_{спр}$ – час спрацьовування тривожної сигналізації;

$t_{вм}$ – час визначення місця доступу;

$t_{бл}$ – час блокування доступу.

Якщо ($T_д$ + $t_{спр}$ + $T_{вм}$ + $t_{бл}$) через $T_{вбл}$, отримаємо співвідношення

$$\frac{T_{вбл}}{t_{п}} < 1, \qquad (4.6)$$

де $T_{вбл}$ – час виявлення та блокування несанкціонованого доступу.

Процес контролю несанкціонованого доступу і несанкціонованих дій порушника представлений на рисунку (рис. 4.2).

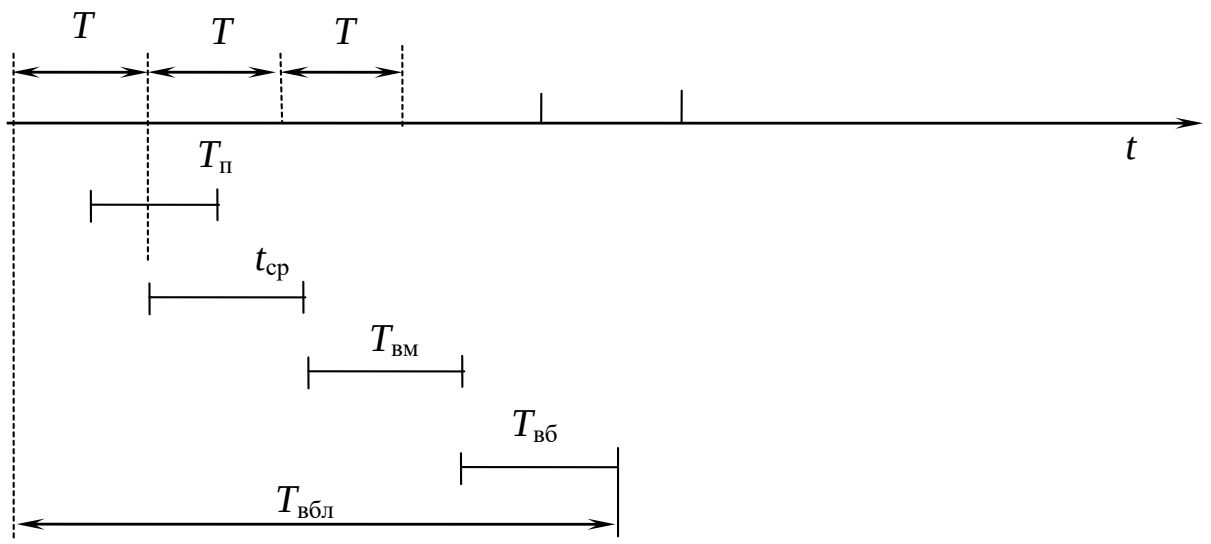


Рис. 4.2. Часова діаграма контролю НСД

З діаграми видно, що порушник може бути не виявлений у двох випадках:

а) коли $t_п < T$;

б) коли $T < t_п < T_{вбл}$;

У першому випадку потрібно додаткова умова – потрапляння інтервалу часу $t_п$ в інтервал Т, тобто необхідна система синхронізація дій порушника з частотою опитування датчиків виявлення. Для вирішення цієї проблеми порушнику доведеться таємно підключити вимірювальну апаратуру в момент виконання НСД, що є досить складним завданням для сторонньої людини. Тому вважаємо, що свої дії з частотою опитування датчиків він синхронізувати не може і доводиться сподіватися на деяку ймовірність попадання відрізка часу $t_п$ в проміжок між імпульсами опитування датчиків, що дорівнює Т.

Згідно з визначенням геометричної ймовірності (курс теорії ймовірності) отримаємо вираз для визначення ймовірності успіху порушника у наступному вигляді.

$$P_{пр} = \frac{T - t_п}{T} = 1 - \frac{t_п}{T}. \qquad (4.7)$$

Ймовірність виявлення несанкціонованого доступу порушника визначається виразом:

$$P_{в} = 1 - P_{пр} \qquad (4.8)$$

або $$P_{в} = \frac{t_{п}}{T}, \qquad (4.9)$$

якщо $t_п > T$ порушник буде виявлений напевно, тобто $T_в = 1$. У другому випадку, коли $T < t_п < T_{вбл}$, ймовірність успіху порушника буде визначатися по аналогії з попереднім співвідношенням:

$$P_{пр} = 1 - \frac{t_{п}}{T_{в.л}}. \qquad (4.10)$$

Ймовірність виявлення і блокування НСД:

$$P_{в.л} = 1 - P_{пр} \qquad (4.11)$$

$$P_{в.л} = \frac{t_{п}}{T_{в.л}}. \qquad (4.12)$$

При $t_п. > T_{вбл}$ спроба несанкціонованого доступу не має сенсу, так як вона буде виявлена.

Таким чином, міцність перешкоди з властивостями виявлення і блокування можна проводити за формулою:

$$P_{ЗЗІ} = P_{вбл} \cup (1\ P_{обх1}) \cup (1\ P_{обх2}) \cup ... \cup (1\ P_{обхj}), \qquad (4.13)$$

де j – число шляхів обходу цієї перешкоди;

$\cup$ – знак «АБО».

Слід зазначити, що ця формула справедлива також і для організаційних заходів захисту.

Для більш повного уявлення про запас міцності перешкоди у вигляді автоматизованої системи виявлення та блокування НСД, необхідно враховувати надійність її функціонування та шляхи можливого її обходу порушником.

Імовірність відмови системи визначається її за формулою:

$$P_{відм}(T) = 1 - e^{-\lambda t}, \qquad (4.14)$$

де λ – інтенсивність відмов групи технічних засобів, що складають систему виявлення і блокування НСД;

t – розглянутий інтервал часу функціонування системи виявлення та блокування несанкціонованого доступу.

З урахуванням можливої відмови системи контролю міцність перешкоди буде:

$$P_{ззіК} = P_{вбл} (1\ P_{відм1}) \cup (1\ P_{обх1}) \cup (1\ P_{обх2}) \cup ... \cup (1\ P_{обхj}), \quad (4.15)$$

де $P_{вбл}$ і $P_{відм}$ визначається за формулами (4.12) і (4.14);

$P_{обх}$ – кількість шляхів обходу j визначається експертним шляхом на основі аналізу принципів побудови системи контролю і блокування несанкціонованого доступу.

Одним з можливих способів обходу системи виявлення та блокування – можливе її відключення або замикання (обриву) контрольних ланцюгів. Таким чином, захисні перешкоди можуть бути двох типів – контрольовані і неконтрольовані людиною. Неконтрольовані визначається за формулою (4.4), а контрольовані (4.15).

Значення $P_{обх1}$, $P_{обх2}$,..., $P_{обхj}$ визначаються в межах від 0 до 1 експертним шляхом на основі досвіду фахівців. При експертній оцінці ймовірності настання тієї чи іншої події ($P_{пр}$, P, $P_{обх}$ і т. ін.) З метою уніфікації методу за основу прийняті такі градації значень:

P = 0 – подія неможлива;

P = 0,2 – подія малоймовірна;

P = 0,5 – подія ймовірна наполовину;

P = 0,8 – подія цілком ймовірна;

P = 0,95 – ймовірність події висока;

P = 1 – подія відбудеться напевно.

Модель багатоланкового захисту. На практиці, у більшості випадків, захисний контур складається кілька «з'єднаних» між собою перешкод з різною міцністю. Модель такого захисту представлена на рис. 4.3. Прикладом такого виду захисту може служити приміщення, в якому зберігається обладнання. Як приклади перешкоди з різною міцністю тут можуть служити стіни, підлога, вікна і замок на дверях тощо.

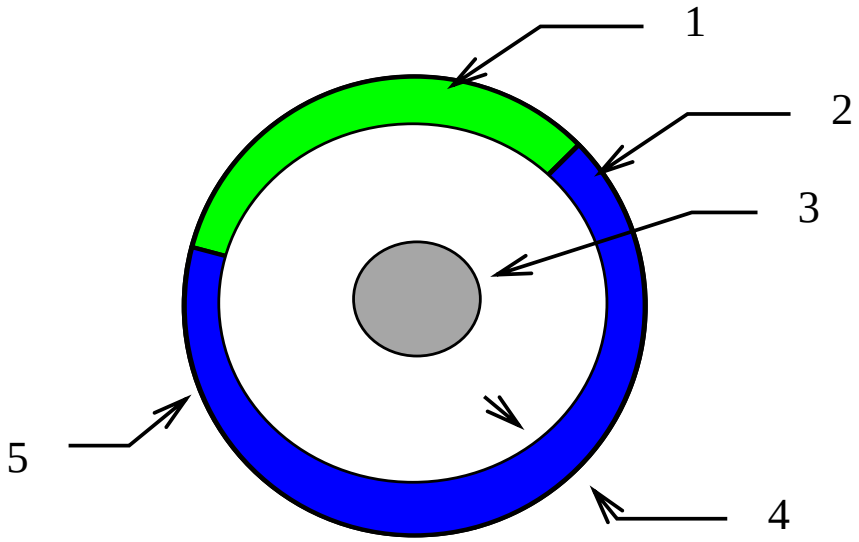


Рис. 4.3. Модель багатоланкового захисту. 1 – перешкода 1; 2 – перешкода 2; 3 – предмет захисту; 4 – міцність перешкоди; 5-перешкода 3

Для обчислювальної системи з'єднання перешкод має дещо іншу реалізацію. Тут слід віднести систему контролю доступу до апаратури, систему захисту від розкриття апаратної складової, систему розпізнавання, систему, яка контролює доступ до периметра комп'ютерної системи. Однак така система не є замкнутим утворенням.

Система не захищена від доступу до засобів відображення інформації, документування, від побічного випромінювання і інших каналів. Таким чином, до складу засобів захисту інформації увійдуть ще система контролю доступу в приміщення, система шифрування тощо. Таким чином, система захисту не буде замкнутою і буде залишатися не захищеною поки є можливість каналів витоку.

Формальний опис для міцності багатоланкового захисту практично збігається з виразами (4.2) і (4.15).

$$P_{ЗЗI} = P_{ззі1} \cup P_{ззі2}\ P_{ззі3} \cup ... \cup P_{ззіі} \cup (1\ P_{обх1}) \cup (1\ P_{обх2}) \cup ... \cdot (1\ P_{обхк}), \qquad (4.16)$$

де $P_{ззіі}$ – міцність і-тої перешкоди.

Вираз для міцності багатоланкового захисту з контрольованими перешкодами матиме вигляд:

$$P_{ззік} = P_{ззік1} \cup P_{ззік2}\ P_{ззік3} \cup ... \cup P_{ззікn} \cup (1\ P_{обх1}) \cup (1\ P_{обх2}) \cup ... \cup (1\ P_{обхj}), \quad (4.17)$$

де $P_{ззікn}$ – міцність n-ої перешкоди.

Тут слід зауважити, що оцінювання міцності інформаційної безпеки для неконтрольованої і контрольованої перешкоди можуть бути роздільними, так як вихідні дані для них різні.

Якщо міцність слабкішої ланки задовольняє висунутим вимогам контуру захисту в цілому, виникає питання про наявність надмірності міцності на всіх інших ланках цього контуру. Тому при проектуванні економічно доцільно використовувати рівноміцні ланки. При розрахунку міцності контуру захисту виникає ситуація, коли ланка з найменшою міцністю не задовольняє висунутим вимогам. У цьому випадку ланку замінюють на більш міцну або її дублюють. Іноді слабка ланка дублюється двома і більше перешкодами. Додаткові перешкоди повинні перекривати ту ж кількість (або більше) можливих каналів НСД, що і перша. Тоді сумарна міцність продубльованих перешкод буде мати вигляд:

$$P_{\Sigma} = 1 - \prod_{i=1}^{m} (1 - P_i), \quad (4.18)$$

де $i = \overline{1, m}$ – порядковий номер перешкоди;

m – кількість дублюючих перешкод;

P_i – міцність і-ї перешкоди.

Ділянку захисного контуру з паралельними (продубльованими) перешкодами іноді називають багаторівневим захистом. У комп'ютерній системі захисні перешкоди часто перекривають одна одну (наприклад, системи контролю доступу в приміщення, охоронної сигналізації та контрольно-пропускного пункту на територію об'єкта захисту).

Багаторівневий захист. У найбільш відповідальних випадках, при підвищених вимогах до систем захисту, застосовується

багаторівневий захист, модель якого представлена на рис. 4.4. Ця модель дозволяє систематизувати роботу зі створення комплексної системи інфобезпеки.

Об'єктами захисту в такій моделі є: інформаційні ресурси, інформаційні процеси і інформація.

Число рівнів захисту комп'ютерної системи або мережі повинно бути не менше чотирьох.

- Зовнішній рівень, що охоплює територію, де розташоване обладнання системи або мережі.
- Рівень споруд, приміщень або пристроїв.
- Рівень компонентів системи (технічних засобів, програмного забезпечення, елементів баз даних).
- Рівень технологічних процесів обробки даних (введення-виведення, внутрішня обробка тощо).

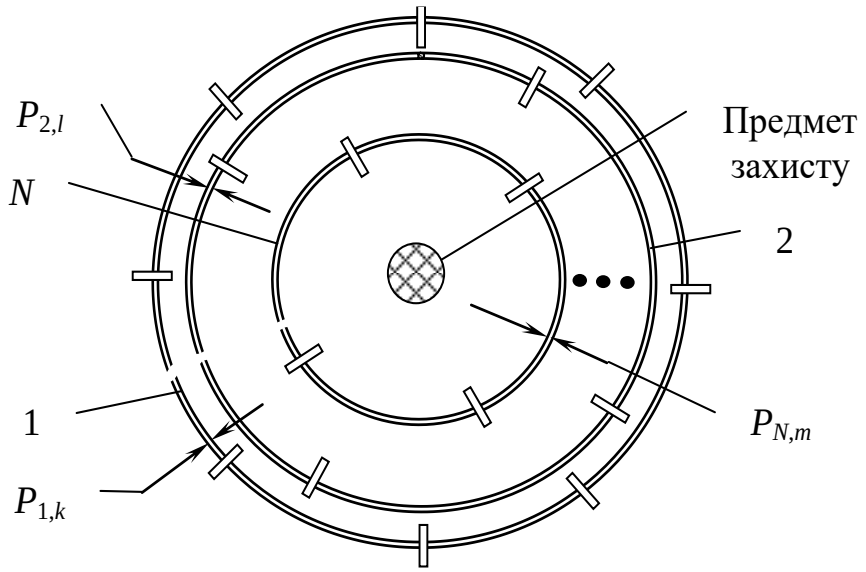


Рис. 4.4. Модель багаторівневого захисту інформації

1, 2,..., N – рівні захисту; $P_{1,\,k}$ – міцність 1-го рівня k-ї ланки; $P_{2,\,l}$ – міцність 2-го рівня l-ї ланки; $P_{N,\,m}$ – міцність N-го рівня m-ї ланки.

При практичній реалізації системного підходу приймають три положення: 1) система захисту і впровадження системи захисту

проводиться одночасно з розробкою комп'ютерної системи; 2) реалізація функції захисту – переважно апаратна; 3) суворе доведення необхідності якраз такого рівня забезпечення захисту.

Міцність багаторівневої системи захисту визначається виразом

$$P_{\Sigma} = 1 - \prod_{n=1}^{N} (1 - P_n), \qquad (4.19)$$

де P_{Σ} – сумарна міцність системи захисту;

P_n – міцність n-го рівня;

N – число рівнів системи захисту.

При $P_N = 0$ цей рівень в розрахунок не береться. При $P_N = 1$ інші рівні є надлишковими. Дана модель справедлива для контурів захисту, що перекривають одні і ті ж канали МКНСД до одного і того ж предмету.

Міцність захисту перешкоди є достатньою, якщо витрати на створення систем захисту адекватні цінності об'єкта захисту і очікуваний час подолання її порушником більше часу життя предмета захисту або більше часу виявлення і блокування його доступу при відсутності шляхів прихованого обходу цієї перешкоди.

При розрахунку сумарної міцності декількох контурів захисту в формулу (4.18) замість P_i включають $P_{кі}$ – міцність кожного контуру, значення якої визначається за однією з формул (4.16) і (4.17), тобто для контрольованих і неконтрольованих перешкод знову розрахунки повинні бути роздільними і проводитися для різних контурів, що утворюють кожну окремий багаторівневий захист. При $P_{кі} = 0$ цей контур в розрахунок не береться. При $P_{кі} = 1$ інші контури є надлишковими. Дана модель справедлива лише для контурів захисту, що перекривають одні і ті ж канали НСД до одного і того ж предмету захисту.

4.2. Концептуальні засади побудови інформаційної безпеки від несанкціонованого доступу в комп'ютерних системах і технологіях

З позицій входу в систему і виходу з неї, відзначимо штатні засоби КС:

- термінали користувачів;
- засоби відображення і документування;
- засоби завантаження програмного забезпечення в систему;
- носії інформації, ОЗП, ДЗП, роздруківки тощо;
- зовнішні канали зв'язку.

Всі перераховані канали називаються штатними каналами, за якими ведеться санкціонований доступ законних користувачів. В даному випадку точки прикладання випадкових впливів розподілені по всій «площі» комп'ютерної системи. Небезпека виникнення випадкових впливів полягає у випадковому спотворенні інформації, що призводять до втрати, модифікації і витоку інформації. Для виявлення та блокування випадкових впливів застосовуються вбудовані в систему засоби функціонального контролю, якісними показниками якого є:

- час виявлення та локалізації відмови;
- достовірність контролю функціонування;
- повнота контролю (охоплення комп'ютерної системи);
- час затримки і виявлення відмови.

Точки прикладання навмисних впливів пов'язані перш за все з входами в систему і виходами інформації з неї, тобто «периметром» системи. Ці входи і виходи можуть бути законними і незаконними тобто:

- всі перераховані штатні засоби при незаконному використанні;
- технологічні пульти і органи управління;
- внутрішній монтаж апаратури;
- лінії зв'язку між апаратними засобами КС;

- побічне електромагнітне випромінювання;
- побічні наведення на мережах електроживлення і заземлення апаратури, допоміжних і сторонніх комунікаціях, розміщених біля КМ;
- зовнішні канали зв’язку.

Небезпека навмисних НСД полягає у введенні порушником незаконних команд, запитів, повідомлень, програм і т. ін., що призводять до втрати, модифікації і НС ознайомлення, а також перехоплення порушником секретної інформації шляхом приймання і спостереження сигналів побічного електромагнітного випромінювання і наведень.

Аналіз КС дозволяє розглядати її як об’єкт, у якому є деяка множина можливих каналів несанкціонованого доступу (МКНСД) до предмету захисту.

Для побудови системи захисту в даній системі на кожному МКНСД, а якщо можливо відразу на декількох необхідно встановити відповідну перешкоду. Чим більша кількість можливих каналів доступу перекрито засобами захисту і їхня ймовірність нездоланність потенційним порушником, тим вище рівень безпеки інформації в КС. Кількість перекриваються МКНСД при цьому буде залежати від заданої кваліфікації порушника. На практиці використовуються наступний розподіл по класах.

1-й клас – всі МКНСД, можливі в даній КС на поточний момент часу.

2-й клас – всі МКНСД, крім машинних носіїв із залишками інформації, що підлягають спеціальній обробці криптографічними методами.

3-й клас – тільки такі МКНСД:

- термінали користувачів;
- апаратура реєстрації та паперові носії інформації;
- засоби завантаження програмного забезпечення;
- технологічні пульти і органи управління;
- внутрішній монтаж апаратури;
- лінії зв’язку між апаратними засобами.

- 4-й клас – тільки такі МКНСД:
- термінали користувачів;
- машинні та паперові документи;
- засоби завантаження програмного забезпечення.

Аналіз можливих каналів НСД показує, що канали діляться на: контрольовані та неконтрольовані перелік яких згадувався раніше. Для забезпечення замикання контуру захисту з декількох різних по виконанню перешкод, недостатньо тільки перекриття всіх можливих каналів НСД. Необхідно ще забезпечити їх взаємодію між собою, тобто об'єднати їх в єдиний постійно діючий механізм. Це завдання виконують централізовані засоби управління.

На контрольованому МКНСД всі ланки і тракти контролю апаратно, програмно і організаційно повинні сходитися на одному робочому місці служби безпеки. Для успішного проектування і розробки системи безпеки необхідно дотримуватися наступного порядку:

1) аналіз заданих вимог до КС на предмет визначення переліку, структури і динаміки вартості оброблюваних даних, що підлягають захисту;

2) вибір моделі потенційного порушника;

3) виявлення в даній КС максимально можливої кількості каналів НСД відповідно до обраної моделі потенційного порушника;

4) аналіз виявлених МКНСД і вибір готових або розробка нових засобів захисту, здатних їх перекриття із заданою міцністю;

5) якісна і кількісна оцінка міцності кожного з застосовуваних засобів захисту;

6) перевірка можливості адаптації засобів захисту в розробляється КС;

7) створення в розробляється КС засобів централізованого контролю і управління;

8) кількісна та якісна оцінка міцності системи інформаційної безпеки в НСД з окремими показниками по контрольованим і неконтрольованим МКНСД.

При створенні захисту необхідно враховувати наступні властивості предмета захисту:

- інформація – об’єкт права власності, що підлягає захисту від несанкціонованого доступу;
- час життя інформації;
- різні джерела, місце і час додатки випадкових і навмисних НСД;
- наявність досить простої моделі потенційного порушника;
- ступінь охоплення КС фундаментальним контролем і засобами підвищення достовірності інформації, які визначають ймовірність появи випадкових НСД;
- можливі канали несанкціонованого доступу до інформації;
- ступінь замикання перешкоди навколо предмета захисту, що визначає ймовірність її обходу порушником;
- розподіл можливих каналів НСД на контрольовані і неконтрольовані;
- залежність міцності перешкоди, що не володіє здатністю контролю несанкціонованого доступу, від здатності перешкоди в своєчасному виявленню та блокування спроб несанкціонованого доступу;
- залежність рівня міцності інформаційної безпеки в КС в цілому від рівня міцності найслабшої ланки;
- можливість створення системи інформаційної безпеки у вигляді єдиного цілого і реально діючого механізму.

Основна тактика і стратегія захисту інформації від несанкціонованого доступу полягає у виконанні наступних завдань:

- попередженні та контролі спроб несанкціонованого доступу;
- своєчасному виявленні місця і блокування несанкціонованих дій;
- реєстрації документування події;
- встановлення і усунення причин несанкціонованого доступу;
- веденні статистики та прогнозуванні несанкціонованого доступу.

Попередження і контроль полягає в:

- застосування засобів функціональної контролю технічних засобів КС і засобів підвищення достовірності інформації;
- для захисту від навмисних НСД створення в КС замкнутого контуру захисту, що складається з системи перешкод, що перекривають максимально можливу кількість каналів НСД і володіють такою міцність, витрати часу на подоланні якої більше часу життя захищається або більше часу виявлення і блокування НСД в ній.

Комп'ютерна система забезпечує безпеку інформації, якщо в ній передбачена централізована система керованих і взаємопов'язаних перешкод, що перекривають з гарантованою міцністю відповідно до моделі потенційного порушника кількість можливих каналів НСД і впливів, спрямованих на втрату або модифікацію інформації, а також несанкціоноване ознайомлення з нею сторонніх осіб.

4.3. Оцінювання ефективності автоматичних засобів управління інформаційною безпекою в комп'ютерних системах і технологіях

Засоби управління інформаційною безпекою виконують цю функцію, будучи важливою складовою частиною засобів захисту. Вони надають допомогу функції контролю, виявлення і блокування НСД, а також безперебійне функціонування апаратних, програмних і організаційних засобів захисту, ведення статистики і прогнозування подій. Всі ці параметри враховуються при оцінці міцності окремих засобів захисту. В результаті оцінювання ефективності засобів управління захистом може проводитися лише з якісної сторони на предмет реалізації захисту як єдиного механізму. Механізм реалізації захисту включає в себе: системи захисту інформації в технічному сенсі, технологію управління,

склад апаратних і програмних засобів управління, організаційних заходів, наявність централізації контролю та управління захистом.

Оцінювання ступеня централізації контролю та управління захистом передбачає оцінку ступеня охоплення окремих засобів захисту засобами контролю і управління. Цей параметр визначає ймовірність обходу захисних перешкод порушником, що встановлюється експертним шляхом. У відповідальних системах всі перешкоди повинні перебувати під централізованим контролем. Оцінювання ефективності засобів управління інформаційною безпекою повинна даватися окремим показником. При цьому важливу роль відіграє ступінь автоматизації контролю функціонування тієї чи іншої захисної перешкоди. Цей показник можна визначити за відношенням кількості перешкод з автоматичною подачею сигналу НСД на централізований засіб контролю, до загальної кількості перешкод, які використовуються в системі інформаційної безпеки в КС. Це відношення можна відображається формулою, що визначає коефіцієнт автоматизації

$$K_A = \frac{N_A}{N}, \qquad (4.20)$$

де k_a – коефіцієнт автоматизації;

N_A – кількість засобів захисту з автоматичною подачею сигналу і блокуванням НСД;

N – загальна кількість засобів інформаційної безпеки в КС.

Таке оцінювання необхідне для визначення ступеня наближення отриманих значень міцності захисту до дійсності. Чим більше автоматизованих засобів захисту, тим менше експертних оцінок і достовірніші результати оцінювання і вище гарантії ефективності захисту.

Тема 5. Засоби інформаційної безпеки в комп'ютерних системах і технологіях

5.1. Розподіл засобів інформаційної безпеки комп'ютерних систем

5.1.1. Розподіл засобів інформаційної безпеки в комп'ютерних мережах

Точки прикладання навмисних впливів пов'язані перш за все з входами в систему і виходами інформації з неї, тобто «периметром» системи. Ці входи і виходи можуть бути законними і незаконними тобто:

- всі перераховані штатні засоби при незаконному використанні;
- технологічні пульти і органи управління;
- внутрішній монтаж апаратури;
- лінії зв'язку між апаратними засобами КС;
- побічне електромагнітне випромінювання;
- побічні наведення на мережах електроживлення і заземлення апаратури, допоміжних і сторонніх комунікаціях, розміщених біля КМ;
- зовнішні канали зв'язку.

Аналіз комп'ютерних систем як об'єкта захисту, можливих каналів несанкціонованого доступу (МКНСД) до інформації обмеженого користування і потенційних загроз дозволяє вибрати і побудувати відповідну систему захисту.

Можливі канали несанкціонованого доступу з боку користувача-порушника вимагають створення на програмному рівні системи розпізнавання та розмежування доступу до інформації з усіма її атрибутами: засобами ідентифікації і

аутентифікації користувачів, розмежування їх повноважень з доступу до файл-сервера і (або) інших суб'єктів даної мережі.

Засоби захисту мережі дозволяють встановлювати право доступу до конкретних каталогів і файлів. При цьому захист даних файл-сервера здійснюється одним способом або в різних поєднаннях чотирма рівнями.

Першим рівнем мережевого захисту є захист даних вхідним паролем, що застосовується по відношенню до всіх користувачів.

Адміністратор безпеки уповноважений здійснювати установку додаткових обмежень із входження в мережу:

- період часу, протягом якого користувач може входити в мережу;
- призначення робочим станціям спеціальних адрес, з якими дозволено входити в мережу;
- обмеження кількості робочих станцій, з яких можна вийти в мережу;
- установка режиму «заборони стороннього втручання», коли при декількох несанкціонованих спробах з невірним паролем встановлюється заборона на вхід в мережу.

Другий рівень захисту даних в мережі – опікунський захист даних при роботі з файлами в заданому каталозі.

Третій рівень захисту даних у каталозі. Кожен каталог має «маску максимальних прав». Обмеження каталогу застосовуються тільки в одному заданому каталозі. Захист в каталозі не поширюється на його підкаталоги.

Четвертий рівень – захист атрибутами файлів використовується в основному для запобігання випадкових змін або видалення окремих файлів. У захисті даних використовуються чотири файлових атрибута: «Запис-Читання/Тільки читання» та «Роздільний/Нероздільний».

Для виключення можливості обходу систем розпізнавання та розмежування доступу в КС і мережах шляхом застосування налагоджувальних програм, а також проникнення комп'ютерних

вірусів, рекомендується їх робота без підключення зовнішніх носіїв інформації.

Потрібно пам'ятати, що наведені рівні захисту будуть виконувати своє завдання, якщо вони становлять замкнутий рівень захисту.

Для розрахунку і оцінювання рівня безпеки інформації в комп'ютерній системі пропонується в залежності від заданої моделі порушника, цінності і важливості оброблюваної інформації використовувати три класи захисту. Розподіл засобів захисту за МКНСД наведений в таблиці 5.1.

Таблиця 5.1

Розподіл засобів захисту за МКНСД

Найменування МКНСД	**Засоби захисту**	**Міцність**	**Клас захисту**		
			I	**II**	**III**
МКНСД елемента мережі (комп'ютера)	Система безпеки інформації елемента мережі (комп'ютера)	G_{PC}	+	+	+
МКНСД сервера	Засоби контролю доступу на територію об'єкта	P_1	+	+	+
	Засоби контролю доступу в приміщення сервера	P_2	+	+	-
	Програма контролю і розмежування доступу до інформації ЛОМ	P_3	+	+	+
	Засоби шифрування	P_4	+	-	-
	Організаційні заходи	P_5	+	+	+

Найменування МКНСД	Засоби захисту	Міцність	Клас захисту		
			I	II	III
МКНСД з боку засобів контролю та управління конфігурацією, адресними таблицями і функціональним контролем ЛОМ	Засоби контролю доступу на територію об'єкта	P_1	+	+	+
	Засоби контролю доступу в приміщення адміністратора	P_2	+	+	-
	Програма розпізнавання і контролю доступу до інформації комп'ютера	P_6	+	+	+
	Програма контролю і розмежування доступу до інформації ЛОМ	P_3	+	+	+
	Засоби контролю цілісності ЛОМ	P_7	+	+	-
МКНСД з боку ліній зв'язку ЛОМ	Засоби контролю доступу на територію об'єкта	P_1	+	+	+
	Організаційні заходи	P_5	+	+	-
	Система шифрування	P_4	+	-	-
МКНСД з боку апаратури передавання даних в канали зв'язку, концентраторів, мостів, комутаторів тощо	Засоби контролю доступу на територію об'єкта	$P_ı$	+	+	+
	Засоби контролю доступу в приміщення	P_2	+	-	-
	Засоби контролю відкривання (розбирання) апаратури	P_8	+	-	-
	Організаційні заходи	P_5	+	+	+
МКНСД до інформації за рахунок ПЕМВН	Засоби контролю доступу на територію об'єкта	P_1	+	-	-
	Засоби зменшення і зашумлення сигналів, що несуть секретну інформацію	P_9	+	-	-

Найменування МКНСД	Засоби захисту	Міцність	Клас захисту		
			I	II	III
МКНСД каналів зв'язку і трактів передавання даних	Засоби захисту в каналах зв'язку	$Р_{кс}$	+	+	+
	Засоби інформаційної безпеки в трактах передавання даних	$Р_{пд}$	+	+	+
МКНСД з боку засобів контролю та управління безпекою інформації в ЛОМ	Засоби контролю доступу на територію об'єкта	$Р_1$	+	+	+
	Засоби контролю доступу в приміщення	$Р_1$	+	+	-
	Програма розпізнавання і контролю доступу до інформації комп'ютера	$Р_6$	+	+	+
	Програма контролю і розмежування доступу до інформації ЛОМ	$Р_3$	+	+	+
	Засоби контролю цілісності ЛОМ	$Р_7$	+	+	-
	Засоби шифрування інформації в комп'ютері	$Р_{10}$	+	-	-
	Засоби шифрування інформації ЛОМ	$Р_4$	+	-	-
	Організаційні заходи	$Р_5$	+	+	+

Дані у таблиці наведені для випадку, де всі приміщення обладнані системою контролю одного типу, а знак «+» означає наявність засобів захисту, знак «-» – відсутність засобів захисту.

5.1.2. Розподіл засобів захисту в моделі взаємозв'язку відкритих систем

Модель процесу взаємодії двох суб'єктів комп'ютерної системи в режимі передавання даних від суб'єкта системи А до суб'єкта В наведена на рис. 5.1.

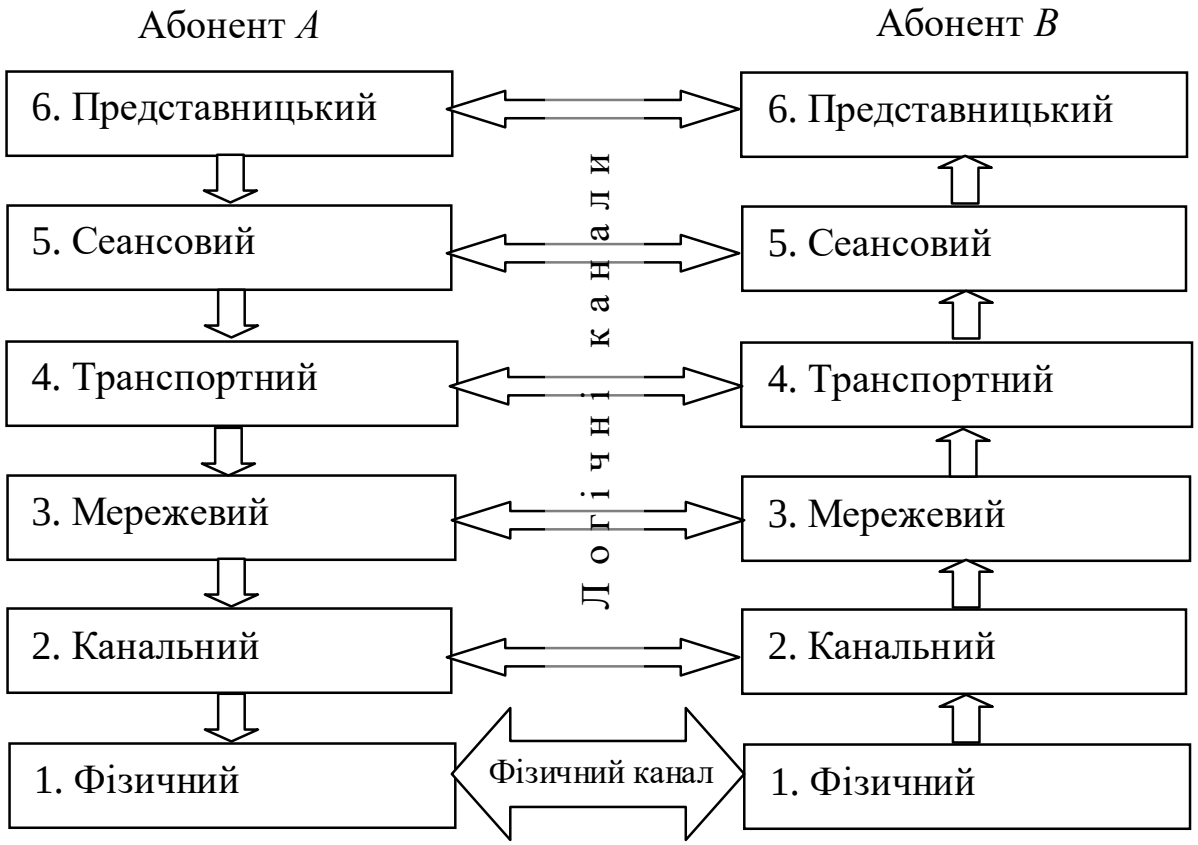


Рис. 5.1. Модель взаємодії рівнів зв'язку OSI

Модель взаємозв'язку відкритих систем складається з 7 рівнів взаємодії компонентів мережі комп'ютерної системи. Безпосередньо дані передаються на передавальному кінці з 7-го до 1-го рівня. На приймальному кінці дані передаються з 1-го до 7-го рівня. На передавальній стороні на кожному з рівнів до переданих даних додається інформація про відповідні рівні, а на приймальній стороні здійснюється витяг інформації відповідного рівня. Таким чином рівні з 7-го по 2-й утворюють логічний канал зв'язку, а 1-й утворює фізичний канал зв'язку. Фізичний канал

зв'язку являє собою фізичне середовище передавання сигналів (кабель, радіоканал, світло та ін.).

Модель взаємозв'язку відкритих систем має наступну ієрархією.

• 7 рівень – прикладний. Це вищий рівень в ієрархії, який забезпечує підтримку прикладних процесів кінцевих користувачів. Він містить всі необхідні елементи сервісу для прикладних програм користувача. На цьому рівні користувач має свої прикладні програми, де може робити все, що йому необхідно, але керується деякими встановленими правилами при обміні з іншими користувачами мережі, тобто повинен виконувати відповідні протоколи.

• 6 рівень – представницький забезпечує перетворення даних користувача до форматів, прийнятих у даній системі; перетворює символьні рядки і коди, організовує файли з метою забезпечення незалежності прикладних програм від форм передавання і отримання даних.

• 5 рівень – сеансовий забезпечує встановлення і підтримку сеансів зв'язку між абонентами при обміні даними, організовує двонаправлений обмін даними з розміщенням в часі, початок і закінчення завдань, відновлення зв'язку після помилок, пов'язаних з відмовою каналу і відмовою мережі взаємодії, відновлює або повторно встановлює з'єднання.

• 4 рівень – транспортний забезпечує управління з'єднанням між різними абонентами, тобто адресацію кінцевих абонентів, а також розбирання та складання повідомлень, збереження блоків даних, доставку даних від вузла до конкретного адресата, приписаного до вузла і навпаки, вибирає маршрут пересилання даних в мережу. Таким чином, транспортний рівень надає послуги сеансовому рівню. Межа між цими рівнями – це межа між власником мережі і користувачем.

Три верхніх рівня є прикладними процесами. Четвертий рівень забезпечує взаємодію між прикладними процесами, встановлюючи між ними логічні канали і забезпечує передачу по цим каналам

інформаційних пакетів (групу байтів, що передаються абонентами мережі один одному), якими обмінюються процеси. Відзначимо, що Internet – це транспортний рівень. Логічні канали, що встановлюються транспортним рівнем, називаються транспортними каналами.

• 3 рівень – мережний, забезпечує інтерфейс кінцевого обладнання даних з мережею комутації пакетів, маршрутизацію пакетів в комунікаційній мережі, межмережеву взаємодію. Мережевий рівень забезпечує функції ретрансляції, відповідно до яких дані направляються по маршруту в потрібному напрямку через пристрої пакетної комутації, тобто до потрібних вузлів згідно з маршрутними таблицями.

• 2 рівень – канальний забезпечує процес передавання даних з інформаційного каналу. Інформаційний канал це логічний канал, який встановлюється між пристроями з'єднаними фізичним каналом. Канальний рівень забезпечує управління потоком даних у вигляді кадрів, виявляє помилки передавання, реалізує алгоритми відновлення інформації у разі виявлення збоїв або втрат даних. Другий рівень розбивається на два підрівні: LLC (Logical Link Control), що забезпечує управління логічною ланкою даних, і MAC (Media Access Control), що забезпечує управління доступом до середовища. Другий підрівень підтримує метод, що забезпечує виконання сукупності правил, за якими вузли мережі отримують доступ до інформаційного ресурсу.

• 1 рівень – фізичний, забезпечує механічні, електричні, функціональні і процедурні засоби для здійснення фізичних з'єднань, їх підтримки та роз'єднання. Середовище поширення сигналів є також фізичним рівнем.

Сервісні служби захисту в відкритих системах та функції які реалізують процедури організації цих служб наведені у таблиці 5.2.

До процедур організації служб або засобів захисту відносяться такі процедури.

Таблиця 5.2

Організація служб інформаційної безпеки

Процедура захисту	Номер процедури	Засіб захисту	Логічні рівні						
			1	2	3	4	5	6	7
Аутентифікація: однорівневих об’єктів джерела даних	1	Шифрування, цифровий підпис	-	-	+	+	-	-	-
		Забезпечення аутентифікації	-	-	+	+	-	-	+
	2	Шифрування	-	-	+	+	-	-	-
		Цифровий підпис	-	-	+	+	-	-	+
Контроль доступу	3	Управління доступом	-	-	+	+	-	-	+
Засекречування: з’єднання в режимі без з’єднання вибіркових полів потоку даних	4	Шифрування	+	+	+	+	-	-	+
		Управління маршрутом	-	-	+	-	-	-	-
	5	Шифрування	-	+	+	+	-	+	+
		Управління маршрутом	-	-	+	-	-	-	-
	6	Шифрування	-	-	-	-	-	+	+
	7	Шифрування	+	-	-	-	-	+	-
		Заповнення потоку	-	-	+	-	-	-	+
		Управління маршрутом	-	-	+	-	-	-	-

Процедура захисту	Номер процедури	Засіб захисту	Логічні рівні						
			1	2	3	4	5	6	7
Забезпечення цілісності:									
з’єднання з відновленням	8	Шифрування, забезпечення цілісності даних	-	-	-	+	-	-	+
з’єднання без відновлення	9	Шифрування, забезпечення цілісності даних	-	-	+	+	-	-	+
вибіркових полів даних	10	Шифрування, забезпечення цілісності даних	-	-	-	-	-	-	+
без встановлення з’єднання даних	11	Шифрування, забезпечення цілісності даних	-	-	+	+	-	-	+
		Цифровий підпис	-	-	-	+	-	-	-
вибіркових полів без з’єднання	12	Цифровий підпис Забезпечення цілісності даних	- -	- -	-	+ -	- -	- -	+ +
інформування:									

Процедура захисту	Номер процедури	Засіб захисту	Логічні рівні						
			1	2	3	4	5	6	7
про відправку	13	Цифровий підпис, забезпечення цілісності даних, підтвердження характеристик даних	-	-	-	-	-	-	+
про доставку	14	Цифровий підпис, забезпечення цілісності даних, підтвердження характеристик даних	-	-	-	-	-	-	+

1. Шифрування даних призначене для закриття всіх даних абонента або деяких полів повідомлення, може мати два рівня: шифрування в каналі зв'язку (лінійне) і міжкінцеве (абонентське) шифрування. У першому випадку, щоб запобігти можливості аналізу трафіка, шифрується вся інформація, передана в канал зв'язку, включаючи всі мережеві заголовки. Абонентське шифрування призначене для запобігання розкриття тільки даних абонента.

2. Цифровий підпис переданих повідомлень служить для підтвердження правильності змісту повідомлення. Він засвідчує факт його відправлення саме тим абонентом, який вказаний в заголовку як джерело даних. Цифровий підпис є функцією від змісту секретного повідомлення, відомого тільки абоненту-джерелу, і загальної інформації, відомої всім абонентам мережі.

3. Управління доступом до ресурсів мережі виконується на підставі множини правил і формальних моделей, що використовують в якості аргументу доступу інформацію про ресурси (класифікацію) і ідентифікатори абонентів. Службова інформація для управління доступом (паролі абонентів, списки дозволених операцій, персональні ідентифікатори, часові обмежувачі тощо) міститься в локальних базах даних служби забезпечення безпеки мережі.

4. Забезпечення цілісності даних передбачає введення в кожне повідомлення деякої додаткової інформації, яка є функцією від змісту повідомлення. У рекомендаціях МОС розглядаються методи забезпечення цілісності двох типів: перші забезпечують цілісність єдиного блоку даних, другі – цілісність потоку блоків даних або окремих полів цих блоків. Ці методи застосовуються у двох режимах – при передаванні даних по віртуальному з'єднанню і при використанні дейтаграмної передачі. У першому випадку виявляються невпорядкованість, втрати, повтори, вставки даних за допомогою спеціальної нумерації блоків або введенням міток часу. У дейтаграмному режимі мітки часу можуть забезпечити тільки обмежений захист цілісності послідовності блоків даних і запобігти переадресації окремих блоків.

5. Процедури аутентифікації призначені для захисту при передаванні в мережі паролів, аутентифікаторів логічних об'єктів тощо. Для цього використовуються криптографічні методи і протоколи, засновані, наприклад, на процедурі «триразового рукостискання». Метою таких протоколів є захист від встановлення з'єднання з логічним об'єктом, утвореним порушником або під його управлінням з метою імітації роботи справжнього об'єкта.

6. Процедура заповнення потоку служить для запобігання можливості аналізу трафіка. Ефективність застосування цієї процедури підвищується, якщо одночасно з нею передбачено лінійне шифрування всього потоку даних, тобто потоки інформації і заповнення робляться нерозрізняючимися.

7. Управління маршрутом призначене для організації передавання даних тільки за маршрутами, утвореними за

допомогою надійних і безпечних технічних пристроїв і систем. При цьому може бути організований контроль з боку одержувача, який у разі виникнення підозри про компрометацію використовуваної системи захисту може зажадати зміни маршруту слідування даних.

8. Процедура підтвердження характеристик даних передбачає наявність арбітра, який є довіреною особою взаємодіючих абонентів і може підтвердити цілісність, час передавання повідомлення, а також запобігти можливості відмови джерела від видачі будь-якого повідомлення, а споживача – від його приймання.

Дані рекомендації з організації служб інформаційної безпеки в комп'ютерних системах і технологіях вимагають більш детального опрацювання на предмет їх реалізації в існуючих протоколах. З позицій запропонованої вище концепції захисту можна помітити деяку надмірність захисних функцій, наприклад аутентифікації, яка є невід'ємною частиною функції контролю доступу і, отже, автоматично до неї входить. Для скорочення кількості засобів захисту доцільно взяти за основу засоби захисту на 7-му рівні і доповнити їх засобами на інших рівнях, але тільки тими, які виконають захисні функції, не охоплені засобами захисту на 7-му рівні.

Для розподілених автоматизованих систем обробки даних: регіональних і глобальних мереж та автоматизованих систем управління через їх високу вартість доцільна класифікація порушника тільки за двома класами: 1- та 2-м, а для локальних – за 1-, 2- і 3-м класом. Засоби захисту, що входять до складу комп'ютерних систем автоматики, можуть забезпечувати захист нижчого класу, а інформація, що передається по каналам зв'язку, повинна бути захищена по тому ж класу. Класифікація потенційного порушника орієнтується на виконання певного набору вимог до безпеки інформації, що передається по каналам зв'язку. Розподіл цих вимог по класам має наступний вигляд:

I клас – всі вимоги;

II клас – всі вимоги, крім приховування факту передавання повідомлення;

III клас – всі вимоги, крім приховування факту передавання повідомлення, гарантованого захисту від ознайомлення з ним сторонньої особи, гарантованої достовірності прийнятих і доставлених даних.

Крім того, для оцінювання ступеня захищеності інформації має значення вихідна позиція порушника по відношенню до об'єкта захисту: поза контрольованою територією – чи є порушник сторонньою особою або на контрольованій території – чи є він законним користувачем, технічним персоналом, який обслуговує комп'ютерну систему. Якщо порушником стає користувач, то для нього не є перешкодою контрольно-пропускний пункт на територію об'єкта захисту, але система контролю доступу в приміщення може дозволити йому доступ тільки в певне приміщення.

Оцінювання захищеності повинна проводитися окремо для кожного випадку. При цьому слід враховувати відповідну кількість МКНСД і засобів захисту. В окремих випадках в необхідно проводити таке оцінювання для кожного користувача.

5.2. Інженерно-технічні засоби захисту

Функціонування будь-якого технічного засобу інформації пов'язано з протіканням по його струмоведучих елементах електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні та електричні поля, які називаються побічними електромагнітними випромінюваннями.

Вузли й елементи електронної апаратури, в яких мають місце великі напруги і протікають малі струми, створюють у ближній зоні електромагнітні поля з переважанням електричної складової. Переважно вплив електричних полів на елементи електронної апаратури спостерігається і в тих випадках, коли ці елементи малочутливі до магнітної складової електромагнітного поля.

Вузли й елементи електронної апаратури, в яких протікають великі струми і мають місце малі перепади напруги, створюють у ближній зоні електромагнітні поля з переважанням магнітної складової. Переважно, вплив магнітних полів на апаратуру спостерігається також у разі, якщо пристрої малочутливі до електричної складової за рахунок властивостей випромінювача. Змінні електричне і магнітне поля створюються в просторі із сполучними лініями (проводами, кабелями) технічних засобів передавання інформації (ТЗПІ).

Побічні електромагнітні випромінювання ТЗПІ є причиною виникнення електромагнітних і параметричних каналів витоку інформації, а також можуть виявитися причиною виникнення наведення інформаційних сигналів в сторонніх струмопровідних лініях і конструкціях. Тому зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня побічного електромагнітного випромінювання і наведень (ПЕМВН) є екранування їх джерел.

Розрізняють електростатичні, магнітостатичні та електромагнітні способи екранування.

Електростатичне і магнітостатичне екранування засноване на замиканні екраном (володіє в першому випадку високою електропровідністю, а у другому – магнітопровідністю) відповідно електричного і магнітного полів.

Електростатичне екранування по суті зводиться до замикання електростатичного поля на поверхню металевого екрана і відведення електричних зарядів на землю (на корпус приладу). Заземлення електростатичного екрана є необхідним елементом при реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля. При використанні діелектричних екранів, які щільно прилягають до екранованого елемента, можна послабити поле джерела наведення у ε раз, де ε – відносна діелектрична проникність матеріалу екрану.

Основним завданням екранування електричних полів є зниження ємності зв’язку між екранованими елементами

конструкції. Ефективність екранування визначається в основному відношенням ємностей зв'язку між джерелом і рецептором наведення до і після установки заземленого екрану. Тому будь-які дії, що призводять до зниження ємності зв'язку, збільшують ефективність екранування.

Екрануюча дія металевого листа істотно залежить від якості з'єднання екрану з корпусом приладу і частин екрану один з одним. Особливо важливо не мати з'єднувальних проводів між частинами екрана і корпусом.

У діапазонах метрових і коротших довжин хвиль сполучні провідники довжиною кілька сантиметрів можуть різко погіршити ефективність екранування. На ще більш коротких хвилях дециметрового і сантиметрового діапазонів сполучні провідники і шини між екранами неприпустимі. Для отримання високої ефективності екранування електричного поля тут необхідно застосовувати безпосереднє суцільне з'єднання окремих частин екрану один з одним.

Вузькі щілини і отвори у металевому екрані, розміри яких малі в порівнянні з довжиною хвилі, практично не погіршують екранування електричного поля.

Зі збільшенням частоти випромінювання ефективність екранування знижується.

Основні вимоги, які пред'являються до електричних екранів, можна сформулювати наступним чином:

- конструкція екрана повинна вибиратися таким чином, щоб силові лінії електричного поля замикалися на стінки екрану, не виходячи за його межі;
- в області низьких частот (при глибині проникнення (b) більше товщини (d), тобто при b > d ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрана з корпусом пристрою і мало залежить від матеріалу екрану і його товщини;

• в області високих частот (при d < b) ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідність і магнітною проникністю.

Магнітостатичне екранування використовується при придушенні наведення на низьких частотах від 0 до 3...10 кГц.

До магнітостатичних екранів пред'являються наступні основні вимоги:

• магнітна проникність μ матеріалу екрану повинна бути якомога вищою. Для виготовлення екранів бажано застосовувати магнітом'які матеріали з високою магнітною проникністю (наприклад, пермаллой);

• збільшення товщини стінок екрану призводить до підвищення ефективності екранування, однак при цьому слід брати до уваги можливі конструктивні обмеження по масі і габаритам екрана;

• стики, розрізи і шви в екрані повинні розміщуватися паралельно лініям магнітної індукції магнітного поля. Їх кількість має бути мінімальною;

• заземлення екрана не впливає на ефективність магнітостатичного екранування.

Ефективність магнітостатичного екранування підвищується при застосуванні багатошарових екранів.

Екранування високочастотного магнітного поля засноване на використанні магнітної індукції, що створює в екрані змінні індукційні вихрові струми (струми Фуко). Магнітне поле цих струмів всередині екрану буде направлено назустріч збуджуючому полю, а за його межами – в ту ж сторону, що і збуджуюче поле. Результуюче поле виявляється ослабленим усередині екрану і посиленим поза ним. Вихрові струми в екрані розподіляються нерівномірно по його перетину (товщині). Це викликається явищем поверхневого ефекту, суть якого полягає в тому, що змінне магнітне поле слабшає в міру проникнення вглиб металу, так як внутрішні шари екрануються вихровими струмами, що циркулюють у поверхневих шарах.

Завдяки поверхневому ефекту щільність вихрових струмів і напруженість змінного магнітного поля в міру поглиблення в метал падає по експоненціальному закону.

Ефективність магнітного екранування залежить від частоти і електричних властивостей матеріалу екрану. Чим нижче частота, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту. Для високих частот, починаючи з діапазону середніх хвиль, (500 кГц і вище) екран з будь-якого металу товщиною 0,5...1,5 мм діє досить ефективно. При виборі товщини і матеріалу екрана слід враховувати механічну міцність, жорсткість, стійкість проти корозії, зручність стиковки окремих деталей і здійснення між ними перехідних контактів з малим опором, зручність пайки, зварювання та ін.

Для частот вище 10 МГц мідна або срібна плівка товщиною більше 0,1 мм дає значний екрануючий ефект. Тому на частотах вище 10 МГц цілком допустимо застосування екранів з фольгованого гетинаксу або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям.

При екрануванні магнітного поля заземлення екрана не змінює величини збуджуючих в екрані струмів і, отже, на ефективність магнітного екранування не впливає.

На високих частотах застосовується виключно електромагнітне екранування. Дія електромагнітного екрану заснована на тому, що високочастотне електромагнітне поле послаблюється їм же створеним (завдяки утворенні у товщі екрану вихрових струмів) полем зворотного напрямку.

Теорія і практика показують, що з точки зору вартості матеріалу і простоти виготовлення переваги на боці екранованого приміщення з листової сталі. Однак при застосуванні сітчастого екрану можуть значно спроститися питання вентиляції та освітлення приміщення. У зв’язку з цим сітчасті екрани також знаходять широке застосування.

Для виготовлення екрана доцільно використовувати такі матеріали:

- сталь листова декапована товщиною (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистова оцинкована товщиною (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистова оцинкована товщиною (мм) 0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;
- сітка сталева ткана номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
- сітка сталева плетена номер 3; 4; 5; 6;
- сітка з латунного дроту марки Л-80 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Металеві листи або полотнища сітки повинні бути між собою електрично з'єднані по всьому периметру. Для суцільних екранів це може бути здійснено електрозварюванням або паянням. Шов електрозварювання або пайки повинен бути безперервним з тим, щоб отримати суцільнозварну конструкцію екрану,

Для сітчастих екранів придатна будь-яка конструкція шва, що забезпечує хороший електричний контакт між сусідніми полотнищами сітки не рідше ніж через 10...15 мм. Для цієї мети може застосовуватися пайка або точкове зварювання.

Екран, виготовлений з лудженої низьковуглецевої сталевої сітки з осередком 2,5...3 мм, дає ослаблення близько 55...60 дБ, а з такою ж подвійною (з відстанню між зовнішньою і внутрішньою сітками 100 мм) – близько 90 дБ. Екран, виготовлений з одинарної мідної сітки з осередком 2,5 мм, дає ослаблення близько 65...70 дБ.

Необхідна ефективність екрану в залежності від його призначення і величини рівня випромінювання ПЕМВН зазвичай знаходиться в межах 60...120 дБ.

Поряд з блоками апаратури, екрануванню підлягають монтажні дроти і сполучні лінії.

Щоб зменшити рівень ПЕМВН, необхідно особливо ретельно виконувати з'єднання оболонки проводу (екрану) з корпусом апаратури. Підключення оболонки має здійснюватися шляхом безпосереднього контакту (найкраще шляхом пайки або зварювання) з корпусом.

Разом з тим з’єднання оболонки проводу з корпусом в одній точці не послаблює в навколишньому просторі магнітне поле, що створюється протікаючим по дроту струмом. Для екранування магнітного поля необхідно створити поле такої ж величини і зворотного напрямку. З цією метою необхідно весь зворотний струм екранованого ланцюга направити через екрануючу обплітку дрота. Для повного здійснення цього принципу необхідно, щоб екрануюча оболонка була єдиним шляхом для протікання зворотного струму.

Висока ефективність екранування забезпечується при використанні витої пари, захищеної екрануючою оболонкою.

На низьких частотах доводиться використовувати більш складні схеми екранування – коаксіальні кабелі з подвійною обпліткою (тріаксільні кабелі).

На більш високих частотах, коли товщина екрана значно перевищує глибину проникнення поля, необхідність у подвійному екрануванні відпадає. У цьому випадку зовнішня поверхня грає роль електричного екрану, а по внутрішній поверхні протікають зворотні струми.

Застосування екрануючої оболонки істотно збільшує ємність між проводом і корпусом, що у більшості випадків небажано. Екрановані дроти більш громіздкі і незручні при монтажі, вимагають запобігання від випадкових з’єднань зі сторонніми елементами і конструкціями.

Довжина екранованого монтажного проводу повинна бути менше чверті довжини найкоротшої хвилі спектра сигналу, що передається по дроту. При використанні більш довгих ділянок екранованих проводів необхідно мати на увазі, що у цьому випадку екранований провід слід розглядати як довгу лінію, яка в уникненні спотворень форми сигналу, що передається, повинна бути навантажена на опір, рівний хвильовому.

Для зменшення взаємного впливу монтажних ланцюгів слід вибирати довжину монтажних високочастотних проводів найменшою, для чого елементи високочастотних схем, пов’язані між собою, слід розміщувати в безпосередній близькості, а

неекрановані проводи високочастотних ланцюгів – при перетині під прямим кутом. При паралельному розташуванні такі дроти повинні бути максимально віддалені один від одного або розділені екранами, в якості яких можуть бути використані несучі конструкції електронної апаратури (кожух, панель тощо).

Екрановані проводи та кабелі слід застосовувати в основному для з'єднання окремих блоків і вузлів один з одним.

Кабельні екрани виконуються у формі циліндра з суцільних оболонок, у вигляді спірально намотаної на кабель плоскої стрічки або у вигляді обплетення з тонкого дроту. Екрани при цьому можуть бути одношаровими і багатошаровими, комбінованими, виготовленими зі свинцю, міді, сталі, алюмінію і їх поєднань (алюміній-свинець, мідь-сталь-мідь і т.ін.).

У кабелях з зовнішніми пластмасовими оболонками застосовують екрани стрічкового типу в основному з алюмінієвих, мідних і сталевих стрічок, накладених спірально або поздовжньо уздовж кабелю.

В області низьких частот корпуси застосовуваних багатоштиркових низькочастотних роз'ємів є екранами і повинні мати надійний електричний контакт із загальною шиною або землею приладу, а зазори між роз'ємом і корпусом повинні бути закриті електромагнітними ущільнювальними прокладками.

В області високих частот коаксіальні кабелі повинні бути узгоджені по хвильовому опору з використовуваними високочастотними роз'ємами. При закладенні коаксіального кабелю у високочастотні роз'єми жила кабелю не повинна мати натягу в місці з'єднання з контактом роз'єму, а сам кабель повинен бути жорстко прикріплений до шасі апаратури поблизу роз'єму.

Для ефективного екранування низькочастотних полів застосовуються екрани, виготовлені з феромагнітних матеріалів з великою відносною магнітною проникністю. При наявності такого екрану лінії магнітної індукції проходять в основному по його стінках, які володіють малим опором у порівнянні з повітряним простором усередині екрану. Якість екранування таких полів залежить від магнітної проникності екрану і опору магнітопровода,

яка буде тим менше, чим товще екран і менше в ньому стиків і швів, що йдуть поперек напрямку ліній магнітної індукції.

Найбільш економічним способом екранування інформаційних ліній зв'язку між пристроями ТЗПІ вважається групове розміщення їх інформаційних кабелів в екрануючий розподільний короб. Коли такого короба немає, то доводиться екранувати окремі лінії зв'язку.

Для захисту ліній зв'язку від наведень необхідно розмістити лінію в екрануючу обплітку або фольгу, заземлену в одному місці, щоб уникнути протікання по екрану струмів, викликаних нееквіпотенціальністю точок заземлення.

Для захисту лінії зв'язку від наведень необхідно мінімізувати площу контуру, утвореного прямим і зворотним проводами лінії. Якщо лінія є одиночним провід, а зворотний струм тече по заземляючій поверхні, то необхідно максимально наблизити провід до поверхні. Якщо лінія утворена двома проводами, то їх необхідно скрутити, утворивши біфіляр (кручену пару). Лінії, виконані з екранованого проводу або коаксіального кабелю, в яких по обплітці протікає поворотний струм, також відповідають вимозі мінімізації площі контуру лінії.

Найкращий захист, як від електричного, так і від магнітного полів забезпечують інформаційні лінії зв'язку типу екранованого біфіляра, тріфіляра (трьох скручених разом проводів, з яких один використовується в якості електричного екрана), тріаксільного кабелю (ізольованого коаксільального кабелю, поміщеного в електричний екран), екранованого плоского кабелю (плоского багатопроводового кабелю, покритого з однієї або обох сторін мідною фольгою).

На рис. 5.2 наведено декілька схем використання на частотах 100 кГц.

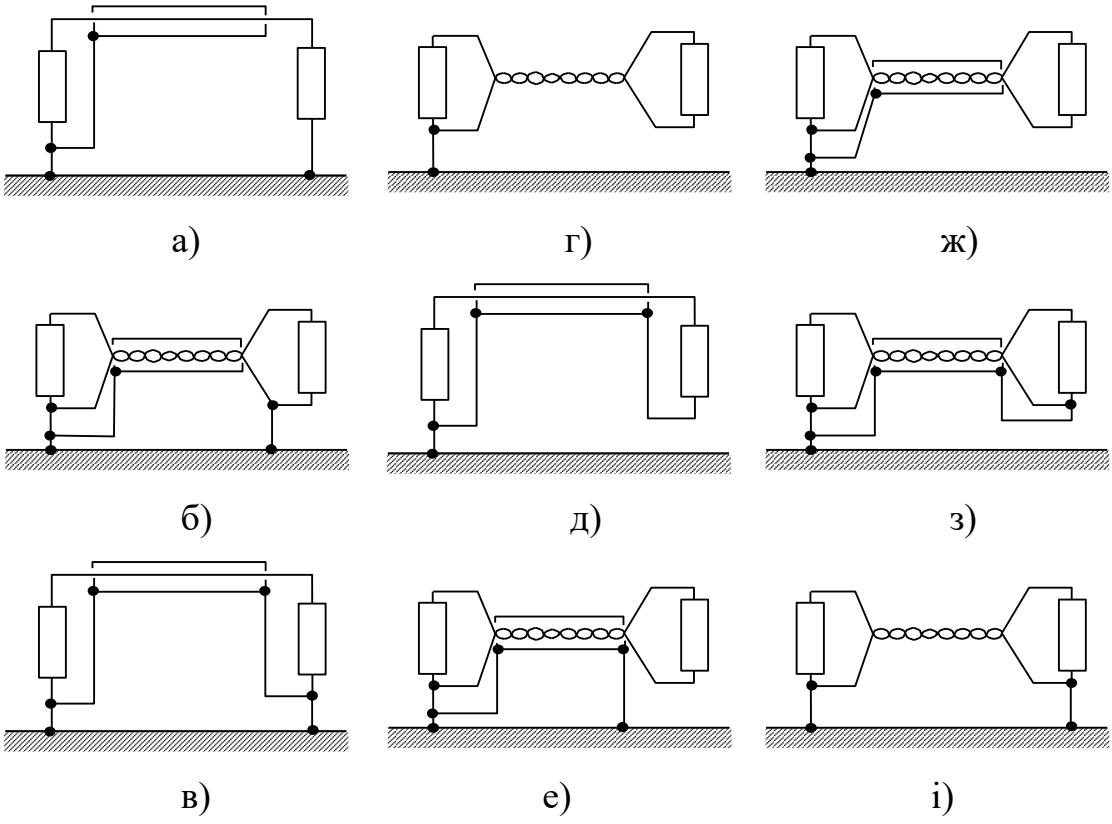


Рис. 5.2. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних і електричних ланцюгів: а) 0 дБ; б) -2 дБ; в) -5 дБ; г) – 49 дБ, кручена пара, 18 витків на метр; д) – 57 дБ; е) – 64 дБ, схема краща на високих частотах; ж) – 64 дБ; з) – 71 дБ; і) – 79 дБ, кручена пара (54 витка на метр)

Схема на рис. 5.2.а, має велику площу петлі, утвореної «прямим» проводом і «землею». Цей ланцюг підвладний, перш за все, магнітному впливу. Екран заземлений на одному кінці і не захищає від магнітного впливу. Перехідне загасання для цієї схеми приймемо рівним 0 дБ для порівняння з загасанням схем на рис. 5.2.б.

Схема на рис. 5.2.б практично не зменшує магнітний зв’язок, так як зворотний провід заземлений з обох кінців, і в цьому сенсі вона аналогічна схемі на рис. 5.2.а. Ступінь поліпшення порівнянна з похибкою розрахунку (вимірювання).

Схема на рис. 5.2.в відрізняється від схеми на рис. 5.2.а наявністю зворотного проводу – коаксіального екрану, проте

екранування магнітного поля погіршено, так як ланцюг заземлений на обох кінцях, в результаті чого з «землею» утворюється петля великої площі.

Схема на рис. 5.2.г дозволяє істотно підвищити захищеність ланцюга (- 49 дБ) завдяки скрутці проводів. У цьому випадку (у порівнянні зі схемою на рис. 5.2.б) петлі немає, оскільки правий кінець ланцюга не заземлений.

Подальше підвищення захищеності ланцюга досягається застосуванням схеми на рис. 5.2.е, коаксіальний ланцюг якої забезпечує краще магнітне екранування, ніж кручена пара на рис. 5.2.г.

Площа петлі в схемі на рис. 5.2.д не більша, ніж у схемі на рис. 5.2.г, так як поздовжня вісь екрану коаксіального кабелю збігається з його центральним проводом.

Схема на рис. 5.2.е дозволяє підвищити захищеність ланцюга завдяки тому, що кручена пара заземлена лише на одному кінці. Крім того, в цій схемі використовується незалежний екран.

Схема на рис. 5.2.ж має ту ж захищеність, що і схема на рис. 5.2.е: ефект той же, що і при заземленні на обох кінцях, оскільки довжина ланцюга і екрану істотно менше робочої довжини хвилі.

Причиною покращення захищеності схеми на рис. 5.2.з у порівнянні з рис. 5.2.ж може бути зменшення площі еквівалентної петлі.

Більш щільне скручування проводів (схема рис. 5.2.і) дозволяє додатково зменшити магнітний зв’язок. Крім того, при цьому зменшується і електричний зв’язок (в обох проводах струми наводяться однаково).

Для зменшення магнітного і електричного зв’язку між проводами необхідно зменшити площу петлі, максимально рознести ланцюги і максимально зменшити довжину паралельного прокладання ліній ТЗПІ і сторонніх провідників.

При нульових рівнях сигналів (0 dB) у сполучних лініях ТЗПІ між ними і сторонніми провідниками має забезпечуватися перехідне загасання не менше 114 dB. Дане перехідне загасання

забезпечується, як правило, при прокладці кабелів ТЗПІ на відстані не менше 0,1 м від сторонніх провідників. При цьому допускається прокладка кабелів ТЗПІ впритул зі сторонніми провідниками при сумарній довжині їх спільного пробігу не більше 70 м.

Екрануватися можуть не тільки окремі блоки апаратури і їх сполучні лінії, а й приміщення в цілому. У звичайних (неекранованих) приміщеннях основний екранувальний ефект забезпечують залізобетонні стіни будинків. Екрануючі властивості дверей і вікон гірші. Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, в тому числі:

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори з металізованої тканини;
- металізоване скло (наприклад, з двоокису олова), що встановлюються в металеві або металізовані рами.

У приміщенні екрануються стіни, двері та вікна.

При закритті дверей повинен забезпечуватися надійний електричний контакт зі стінками приміщення (з дверною рамою) по всьому периметру не рідше ніж через 10...15 мм. Для цього може бути застосована пружинна гребінка з фосфористої бронзи, яку зміцнюють по всьому внутрішньому периметру дверної рами.

Вікна повинні бути затягнуті одним або двома шарами мідної сітки з вічком не більше 2 * 2 мм, причому відстань між шарами сітки має бути не менше 50 мм. Обидва шари сітки повинні мати хороший електричний контакт зі стінками приміщення (з рамою) по всьому периметру. Сітки зручніше робити зйомними і металеве обрамлення зйомної частини також має мати пружні контакти у вигляді гребінки з фосфористої бронзи.

При проведенні робіт з ретельного екранування подібних приміщень необхідно одночасно забезпечити нормальні умови для працюючої в ньому людини, перш за все вентиляцію повітря і освітлення.

Конструкція екрану для вентиляційних отворів залежить від діапазону частот. Для частот менше 1000 МГц застосовуються

стільникові конструкції, що закривають вентиляційний отвір, з прямокутними, круглими, шестигранними отворами. Для досягнення ефективного екранування розміри осередків повинні бути менше однієї десятої від довжини хвилі. При підвищенні частоти необхідні розміри осередків можуть бути настільки малими, що погіршується вентиляція.

Екранування електромагнітних хвиль понад 100 дБ можна забезпечити тільки в спеціальних екранованих камерах, у яких електромагнітний екран виконаний у вигляді електрогерметичного сталевого корпусу, а для введення електричних комунікацій використовуються спеціальні фільтри.

Розміри екранованого приміщення вибирають виходячи з його призначення і вартості. Зазвичай екрановані приміщення будують площею 5...8 м^2 при висоті 2,5...3 м.

Необхідно пам’ятати, що екранування ТЗПІ та з’єднувальних ліній ефективно тільки при правильному їх заземленні. Тому одним з найважливіших умов щодо захисту ТЗПІ є правильне заземлення цих пристроїв.

В наш час існують різні типи заземлень. Найбільш часто використовуються одноточкові, багатоточкові і комбіновані (гібридні) схеми.

На рис. 5.3 представлена одноточкова послідовна схема заземлення.

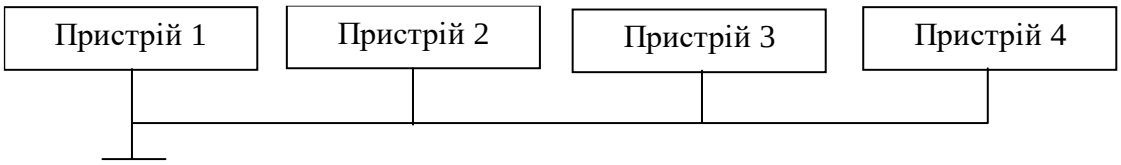


Рис. 5.3. Одноточкова послідовна схема заземлення

Ця схема найбільш проста, але має недолік, пов’язаний з протіканням зворотних струмів різних ланцюгів за спільною ділянкою заземляючого ланцюга з можливістю появи небезпечного сигналу в сторонніх ланцюгах.

У одноточкової паралельної схеми заземлення (рис. 5.4) цього недоліку немає. Однак така схема вимагає великого числа заземлюючих провідників, через що може виникнути проблема із забезпеченням малого опору заземлення ділянок ланцюга. Крім того, між заземлювальними провідниками можуть бути небажані зв'язки, які створюють кілька шляхів заземлення для кожного пристрою. В результаті в системі заземлення можуть виникнути зрівнювальні струми і з'явитися різниця потенціалів між різними пристроями.

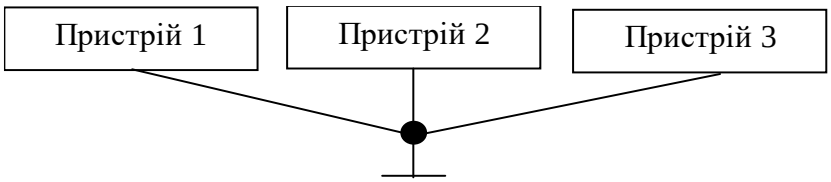


Рис. 5.4. Одноточкова паралельна схема заземлення

Багатоточкова схема заземлення (рис. 5.5) практично вільна від недоліків, властивих одноточковій схемі.

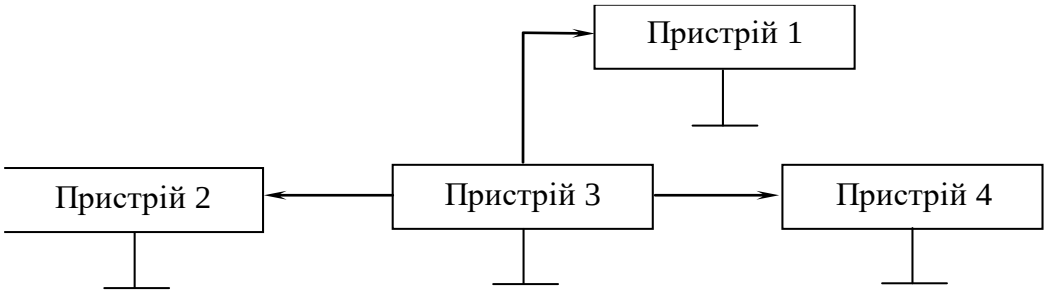


Рис. 5.5. Багатоточкова схема заземлення

У цьому випадку окремі пристрої і ділянки корпусу індивідуально заземлені. При проектуванні і реалізації багатоточкової системи заземлення необхідно вживати спеціальних заходів для виключення появи замкнутих контурів.

Як правило, одноточкове заземлення застосовується на низьких частотах при невеликих розмірах заземлюючих пристроїв

та відстанях між ними менше 0,5 • λ. На високих частотах при великих розмірах заземлюючих пристроїв та значних відстанях між ними використовується багатоточкова система заземлення. У проміжних випадках ефективна комбінована (гібридна) система заземлення, що представляє собою різні поєднання одноточкової, багатоточкової і плаваючої заземлюючих систем.

Заземлення технічних засобів комп'ютерних систем та систем зв'язку повинно бути виконано відповідно до певних правил.

Основні вимоги, що пред'являються до системи заземлення:

- система заземлення повинна включати загальний заземлювач, кабель заземлення, шини і дроти, що сполучають заземлювач з об'єктом;
- опір заземлюючих провідників і шин повинні бути мінімальними;
- кожен заземлюючий елемент повинен бути приєднаний до заземлювача або до заземлювальної магістралі за допомогою окремого відгалуження. Послідовне включення в заземлюючий провідник декількох заземлюючих елементів забороняється;
- в системі заземлення мають бути відсутні замкнуті контури, утворені сполуками або небажаними зв'язками між сигнальними ланцюгами і корпусами пристроїв, між корпусами пристроїв і землею;
- слід уникати використання загальних провідників в системах екрануючого заземлення, захисних заземлень і сигнальних ланцюгів;
- якість електричних з'єднань в системі заземлення має забезпечувати мінімальний опір контакту, надійність і механічну міцність контакту в умовах кліматичних впливів і вібрації;
- контактні з'єднання повинні виключати можливість утворення оксидних плівок на контактуючих поверхнях і пов'язаних з цими плівками нелінійних явищ;
- контактні з'єднання повинні виключати можливість утворення гальванічних пар для запобігання корозії в ланцюгах заземлення;

• забороняється використовувати в якості заземлюючого пристрою нульові фази електромереж, металоконструкції будівель, що мають з'єднання з землею, металеві оболонки підземних кабелів, металеві труби систем опалення, водопостачання, каналізації тощо.

Опір заземлення визначається головним чином опором розтікання струму в землі. Величину цього опору можна значно знизити за рахунок зменшення перехідного опору між заземлювачем і ґрунтом шляхом ретельного очищення перед укладанням поверхні заземлювача і утрамбовкою навколо нього ґрунту, а також підсипанням кухонної солі.

Таким чином, величина опору заземлення буде в основному визначатися опором ґрунту.

Питомий опір різних ґрунтів (тобто електричний опір 1 $см^3$ ґрунту) залежить від вологості ґрунту, його складу, щільності, температури і т. ін., і коливається в дуже широких межах (див. табл. 5.3).

Таблиця 5.3

Значення питомої опору різних ґрунтів

Тип ґрунту	Питомий опір (р), Ом/$см^3$		
	середній	мінімальний	максимальний
Золи, шлаки, соляні відходи	2370	500	7000
Глина, суглинки, сланці	4060	340	16300
Те ж з домішками піску	15800	1020	135 000
Гравій, пісок, каміння з невеликою кількістю глини або суглинків	94000	59000	458 000

Ґрунти втрачають свої властивості з провідності при відсутності вологи. Для більшості ґрунтів 30% вмісту вологи достатньо для забезпечення малого опору. Наприклад, для

суглинків питомий опір при вологості 5% становить 165000 Ом/см^3, а при вологості 30% – 6400 Ом/см^3.

При промерзанні опір ґрунтів різко зростає. Наприклад, для суглинків питомий опір при вологості 15% і температурі 20°С становить 7200 Ом/см^3, при температурі -5°С – 79000 Ом/см^3, а при температурі -15°С – 330000 Ом/см^3.

Зрошення ґрунту навколо заземлювачів 2...5 процентним соляним розчином значно (в 5...10 разів) знижує опір заземлення.

Врахувати всі фактори, що впливають на провідність ґрунту, аналітичним шляхом практично неможливо, тому при влаштуванні заземлення величину питомого опору ґрунту в тих місцях, де передбачається розміщення заземлення, визначають дослідним шляхом.

Як правило, вимірювання опору заземлення проводиться два рази на рік (взимку і влітку).

Якщо заземлювач складається з металевої пластини радіуса r, розташованої безпосередньо біля поверхні землі, то опір заземлення $R_З$ можна розрахувати за формулою

$$R_З = \frac{\rho}{4r_П}, \text{ Ом,} \qquad (5.1)$$

де ρ – питомий опір ґрунту, Ом/см^3;

$r_п$ – радіус пластини, см.

При збільшенні глибини закапування $l_З$ пластини опір заземлення зменшується і при $l_З$ значно більше r ($l_З$»r) величина $R_З$ зменшується в два рази.

Досить часто застосовують заземлюючі пристрої у вигляді вертикально вбитої труби. Опір заземлення в цьому випадку визначається формулою

$$R_З = \frac{\rho}{2\pi l}\left[\ln\left(\frac{4l}{r_Т} - 1\right)\right], \text{ Ом,} \qquad (5.2)$$

де l – довжина труби, см;

$r_Т$ – радіус труби, см.

З формули видно, що опір заземлення залежить більшою мірою не від радіуса труби, а від її довжини. Тому при влаштуванні заземлення доцільніше застосовувати тонкі й довгі труби (стрижні з арматури).

У табл. 5.4. наведені експериментально отримані значення опору заземлення стрижневого заземлювача (Ø 15,9 мм, l = 1,5 м) для різних ґрунтів.

У якості одиночних стрижневих заземлювачів доцільно використовувати мідні заземлювальні стрижні.

Як видно з табл. 5.4, опір простих одиночних заземлювачів виявляється досить великим. Тому такі заземлювачі знаходять застосування при невисоких вимогах до заземлюючих пристроїв або при ґрунтах з дуже великою провідністю.

Таблиця 5.4

Значення опору заземлення стрижневого заземлювача (Ø15,9 мм, L = 1,5 м) для різних ґрунтів

Тип ґрунту	Опір заземлення $R_З$, Ом		
	середній	мінімальний	максимальний
Золи, шлаки, соляні відходи	14	3,5	41
Глина, суглинки, сланці	24	2	98
Те ж з домішками піску	93	6	800
Гравій, пісок, каміння з невеликою кількістю глини або суглинків	554	35	2700

При підвищених вимогах до величини опору заземлення (опір заземлення ТЗПІ не повинен перевищувати 4 Ом) застосовують багаторазове заземлення, що складається з ряду одиночних симетрично розташованих заземлювачів, з’єднаних між собою.

На практиці найбільш часто в якості заземлювачів застосовують:

- стрижні з металу, що мають високу електропровідність, занурені в землю і з'єднані з наземними металевими конструкціями засобів ТЗПІ;
- сіткові заземлювачі, виготовлені з елементів мають високу електропровідність і занурені в землю (служать в якості доповнення до заземлюючих стержнів).

При необхідності влаштування високочастотного заземлення потрібно враховувати не тільки геометричні розміри заземлювачів, їх конструкцію і властивості ґрунту, але і довжину хвилі високочастотного випромінювання. Сумарний високочастотний опір заземлення Z_S складається з високочастотного опору магістралі заземлення Z_M (дроту, що йде від заземлюючого пристрою до поверхні землі) і з високочастотного опору самого заземлювача Z_S (дроту, металевого стрижня або листа, що знаходиться в землі).

Величина заземлення в основному визначається не опором заземлення, а опором заземляючої магістралі. Для зменшення опору слід прагнути перш за все до зменшення індуктивності заземляючої магістралі, що досягається за рахунок зменшення її довжини і виготовлення магістралі у вигляді стрічки, яка має в порівнянні з проводом круглого перетину меншу індуктивність. У тих випадках, коли індуктивність заземляючої магістралі можна зробити дуже малою або використовувати її для отримання послідовного резонансу при блокуванні випромінюючих мереж захисними конденсаторами на землю (наприклад, при комплексному придушенні випромінювання в приміщеннях), доцільно значно зменшити величину опору заземлення Z_S. Зменшити величину Z_S можна також багаторазовим заземленням з симетрично розташованих заземлювачів.

При цьому загальний опір заземлення буде тим менше, чим далі один від одного розташовані окремі заземлювачі.

При влаштуванні заземлення в якості заземлювачів найчастіше застосовуються сталеві труби довжиною 2...3 м і діаметром 35...50 мм і сталеві смуги перетином 50...100 мм.

Найбільш придатними є труби, що дозволяють досягти глибоких і найбільш вологих шарів землі, що володіють найбільшою провідністю і не піддаються висиханню або промерзанню. Однак тут необхідно враховувати, що зі зменшенням опору ґрунту зростає корозія металу. Крім того, застосування таких заземлювачів не пов'язане зі значними земляними роботами, що неминуче, наприклад, при виконанні заземлення з металевих листів або металевих стрічок і проводів, що горизонтально закладаються в землю.

Заземлювачі слід з'єднувати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення за умовами механічної міцності і отримання достатньої провідності рекомендується брати не менше (24 х 4) мм^2. Провідник, що з'єднує заземлювач з контуром заземлення, повинен бути лудженим для зменшення гальванічної корозії, а з'єднання повинні бути захищені від впливу вологи.

Магістралі заземлення поза будівлею необхідно прокладати на глибині близько 1,5 м, а всередині будівлі – по стіні або спеціальних каналах таким чином, щоб їх можна було оглядати зовні. З'єднують магістралі з заземлювачем тільки за допомогою зварювання. До заземлюючих пристроїв ТЗПІ магістраль підключають за допомогою болтового з'єднання в одній точці.

Для зменшення опорів контактів найкращим є постійне безпосереднє з'єднання металу з металом, отримане зварюванням або паянням. При з'єднанні під гвинт необхідно застосовувати шайби (зірочки або Гровера), що забезпечують сталість щільності з'єднання.

При контакті двох металів у присутності вологи виникає гальванічна і (або) електрична корозія. Гальванічна корозія є наслідком виникнення гальванічного елемента, в якому волога є електролітом. Ступінь корозії визначається положенням цих металів в електричному ряду. Електрична корозія може виникнути при контакті в електроліті двох однакових металів. Вона визначається наявністю локальних електрострумів у металі, наприклад, струмів у заземленнях силових ланцюгів. Найбільш

ефективним методом захисту від корозії є застосування металів з малою електрохімічною активністю, таких, як олово, свинець, мідь. Значно зменшити корозію і забезпечити хороший контакт можна, ретельно ізолюючи з'єднання від проникнення вологи.

Одним з методів локалізації небезпечних сигналів, що циркулюють в технічних засобах і системах обробки інформації, є фільтрація. У джерелах електромагнітних полів і наведень фільтрація здійснюється з метою запобігання поширенню небажаних електромагнітних коливань за межі пристрою – джерела небезпечного сигналу. Фільтрація в пристроях – рецепторах електромагнітних полів і наведень повинна виключити їх вплив на рецептор.

Для фільтрації сигналів в ланцюгах живлення ТЗПІ використовуються розділові трансформатори і перешкодопридушуючі фільтри.

Розділові трансформатори повинні забезпечувати розв'язку первинного та вторинного ланцюгів за сигналами наводки. Це означає, що у вторинний ланцюг трансформатора не повинні проникати наведення, що з'являються в ланцюзі первинної обмотки. Проникнення наведень у вторинну обмотку пояснюється наявністю небажаних резистивних і ємнісних ланцюгів зв'язку між обмотками. Для зменшення зв'язку обмоток за сигналами наведень часто застосовується внутрішній екран, що виконується у вигляді заземленої прокладки або фольги, що укладається між первинною і вторинною обмотками. За допомогою цього екрана наводка, що діє у первинній обмотці, замикається на землю. Однак електростатичне поле навколо екрану також може служити причиною проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються з метою вирішення ряду завдань, у тому числі для:

- поділу за ланцюгами живлення джерел і рецепторів наведення, якщо вони підключаються до одних і тих же шин змінного струму;
- усунення асиметричних наведень;

• ослаблення симетричних наведень в ланцюзі вторинної обмотки, обумовлених наявністю асиметричних наведень в ланцюзі первинної обмотки.

Засоби розв'язки та екранування, що застосовуються в розділових трансформаторах, забезпечують максимальне значення опору між обмотками і створюють для наведень шлях з малим опором з первинної обмотки на землю. Це досягається забезпеченням високого опору ізоляції відповідних елементів конструкції (~ 104 МОм) і незначною ємністю між обмотками. Зазначені особливості трансформаторів для ланцюгів живлення забезпечують більш високу ступінь придушення наведень, ніж звичайні трансформатори.

Розділовий трансформатор зі спеціальними засобами захисту і розв'язки забезпечує ослаблення інформаційного сигналу наведення в навантаженні на 126 дБ при ємності між обмотками 0,005 пФ і на 140 дБ при ємності між обмотками 0,001 пФ.

Засоби екранування, що застосовуються в розділових трансформаторах, повинні не тільки усувати вплив асиметричних наведень на захищається пристрій, але і не допустити на виході трансформатора симетричних наведень, обумовлених асиметричними наведеннями на його вході. Застосовуючи в розділових трансформаторах спеціальні засоби екранування, можна істотно (більш ніж на 40 дБ) зменшити рівень таких наведень.

Перешкодопридушуючі фільтри. В наш час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів в різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові і загороджувальні фільтри тощо. Основне призначення фільтрів – пропускати без значного ослаблення сигнали з частотами, що лежать в робочій смузі частот, і пригнічувати (послаблювати) сигнали з частотами, що лежать за межами цієї смуги.

Для виключення просочування інформаційних сигналів у колі електроживлення використовуються фільтри нижніх частот.

Фільтр нижніх частот (ФНЧ) пропускає сигнали з частотами нижче граничної частоти ($f \leq f_{гр}$) і придушує – з частотами вище граничної частоти.

Послідовна гілка ФНЧ повинна мати малий опір для постійного струму і нижніх частот. Разом з тим для того, щоб вищі частоти затримувалися фільтром, послідовний опір має зростати з частотою. Цим вимогам задовольняє індуктивність L.

Паралельна гілка ФНЧ, навпаки, повинна мати малу провідність для низьких частот з тим, щоб струми цих частот шунтуватися паралельним плечем. Для високих частот паралельна гілка повинна мати більшу провідність, тоді коливання цих частот будуть нею шунтуватися, і їх струм на виході фільтра буде послаблюватися. Таким вимогам відповідає ємність С.

Більш складні багатоланкові ФНЧ (Чебишева, Баттерворта, Бесселя і ін.) конструюють на основі поєднань різних одиничних ланок.

Кількісно величина ослаблення (фільтрації) небажаних (в тому числі і небезпечних) сигналів захисним фільтром оцінюється відповідно до виразу:

$$A = 20\lg\left(\frac{U_1}{U_2}\right) = 10\lg\left(\frac{P_1}{P_2}\right), \text{ ДБ,} \qquad (5.3)$$

де U_1 (P_1) – напруга (потужність) небезпечного сигналу на вході фільтра;

U_2 (P_2) – напруга (потужність) небезпечного сигналу на виході фільтра при включеному навантаженні $Z_Н$.

Основні вимоги, що пред’являються до захисних фільтрів, полягають у наступному:

- величини робочої напруги і струму фільтра повинні відповідати напрузі і струму фільтрованого ланцюга;
- величина ослаблення небажаних сигналів у діапазоні робочих частот повинна бути не менше необхідної;
- ослаблення корисного сигналу в смузі прозорості фільтра має бути незначним;

- габарити і маса фільтрів повинні бути мінімальними;
- фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) і механічних навантажень (удари, вібрація і т.ін.);
- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

До фільтрів ланцюгів живлення поряд із загальними пред'являються такі додаткові вимоги:

- загасання, що вноситься фільтрами в ланцюзі постійного струму або змінного струму основної частоти, має бути мінімальним (наприклад, 0,2 дБ і менше) і мати велике значення (більш 60 дБ) у смузі придушення, яка в залежності від конкретних умов може бути до 10 ГГц;
- мережеві фільтри повинні ефективно працювати при великих значеннях струму, високих напругах і значних рівнях потужності електромагнітних коливань, що проходять і затримуються фільтром;
- обмеження, що накладаються на допустимі рівні нелінійних спотворень форми напруги живлення при максимальному навантаженні, повинні бути досить жорсткими (наприклад, рівні гармонійних складових напруги живлення з частотами вище 10 кГц повинні бути на 80 дБ нижче рівня основної гармоніки).

Напруга, прикладена до фільтру, має бути такою, щоб вона не викликало пробою конденсаторів фільтра при різних скачках напруги живлення, включаючи стрибки, обумовлені перехідними процесами в ланцюгах живлення. Щоб при заданих масі і об'ємі, фільтр забезпечував найкраще придушення наведень у необхідному діапазоні частот, його конденсатори повинні мати максимальну ємність на одиницю об'єму або маси. Крім того, номінальне значення робочої напруги конденсаторів вибирають виходячи з максимальних значень допустимих стрибків напруги мережі живлення.

Струм через фільтр повинен бути таким, щоб не виникало насичення сердечників котушок фільтра. Крім того, слід

враховувати, що зі збільшенням струму через котушку збільшується реактивне падіння напруги на ній. Це може привести до:

- погіршення еквівалентного коефіцієнта стабілізації напруги в мережі живлення, що містить фільтр;
- виникненню взаємозалежності перехідних процесів у різних навантаженнях ланцюга живлення.

Найбільші коливання напруги при цьому виникають під час відключення навантажень, так як більшість з них має індуктивний характер.

Характеристики фільтрів залежать від числа використаних реактивних елементів. Так, наприклад, фільтр з одного паралельного конденсатора або однієї послідовної індуктивної котушки може забезпечити загасання лише 20 дБ/декада поза смугою пропускання, а LC – фільтр з десяти або більше елементів – понад 200 дБ/декада.

Через паразитний зв’язок між входом і виходом фільтра на практиці важко отримати загасання більше 100 дБ. Якщо фільтр неекранований і сигнал подається на нього і знімається за допомогою неекранованих з’єднань (проводів), то розв’язка між входом і виходом зазвичай не перевищує 40...60 дБ. Для забезпечення розв’язки більше 60 дБ необхідно використовувати екрановані фільтри з роз’ємами і використовувати для з’єднання екрановані дроти.

Фільтри з гарантованим загасанням 100 дБ виконуються у вигляді вузла з електромагнітним екрануванням, який поміщається в корпус, виготовлений з матеріалу з високою магнітною проникністю магнітного екрану. Цим суттєво зменшується можливість виникнення всередині корпусу паразитного зв’язку між входом і виходом фільтра через магнітні, електричні або електромагнітні поля.

Через вплив паразитних ємностей і індуктивностей фільтр часто не забезпечує необхідного загасання на частотах, що перевищують граничну частоту (f_C) на дві декади, і цілком може

втратити працездатність на частотах, що перевищують граничну частоту на кілька декад.

Орієнтовні значення максимального загасання для мережевих фільтрів, наведені в табл. 5.5.

Таблиця 5.5

Значення максимального загасання для мережевих фільтрів

Діапазон Частот	**Максимальне загасання фільтра поза смугою пропускання, дБ**		
	екранований		**неекранований**
	з роз'ємами	без роз'ємів	
Фільтри в ланцюгах живлення на струми не більше 10 А			
$f_c \leq f \leq 10\ f_c$	80	-	-
$10\ f_c \leq f \leq 100\ f_c$	80	-	-
$f > 100\ f_c$	70	-	-
Фільтри в ланцюгах живлення на струми більше 1 0 А			
$f_c \leq f \leq 10\ f_c$;	100	-	-
$10\ f\,c \leq f \leq 100\ f_c$	100	-	-
$f > 100\ f_c$	90	-	-

Конструктивно фільтри підрозділяються на:

- фільтри на елементах з зосередженими параметрами (LC-фільтри) – зазвичай призначені для роботи на частотах до 300 МГц;
- фільтри з розподіленими параметрами (смугові, коаксіальні або хвильові) – застосовуються на частотах понад 1 ГГц;
- комбіновані фільтри застосовуються на частотах 300 МГц...1 ГГц.

Реалізація пасивних методів захисту, заснованих на застосуванні екранування і фільтрації, призводить до ослаблення рівнів побічних електромагнітних випромінювань і наведень (небезпечних сигналів) ТЗПІ і тим самим до зменшення відношення

небезпечний сигнал/шум (с/ш). Однак в ряді випадків, незважаючи на застосування пасивних методів захисту, на межі контрольованої зони відношення с/ш перевищує допустиме значення, і тому, застосовуються активні заходи захисту, засновані на створенні перешкод засобам розвідки, що призводить до зменшення відношення с/ш.

Для виключення перехоплення побічних електромагнітних випромінювань по електромагнітному каналу використовується просторове зашумлення, а для виключення знімання наведень інформаційних сигналів з сторонніх провідників і сполучних ліній – лінійне зашумлення.

До системи просторового зашумлення, що застосовується для створення маскувальних електромагнітних перешкод, висуваються такі вимоги:

- система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;
- створювані перешкоди не повинні мати регулярної структури;
- рівень створюваних перешкод (як по електричній, так і по магнітній складовій поля) повинен забезпечити ставлення с/ш на межі контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;
- система повинна створювати перешкоди як з горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);
- на межі контрольованої зони рівень перешкод, що створюються системою просторового зашумлення, не повинен перевищувати встановлених норм щодо електромагнітної сумісності (ЕМС).

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечний сигнал/шум на межі контрольованої зони не перевищує деякого допустимого значення, що розраховується за спеціальними методиками для кожної частоти інформаційного

(небезпечного) побічного електромагнітного випромінювання ТЗПІ.

У системах просторового зашумлення в основному використовуються перешкоди типу «білого шуму» або «синфазних перешкод».

Системи, що реалізують метод «синфазної перешкоди», в основному застосовуються для захисту комп'ютера. У них в якості перешкодного сигналу використовуються імпульси випадкової амплітуди, що збігаються (синхронізовані) за формою і часу існування з імпульсами корисного сигналу. Внаслідок цього за своїм спектральним складом перешкодний сигнал аналогічний спектру побічних електромагнітних випромінювань комп'ютера. Тобто, система зашумлення генерує «імітаційну перешкоду», що за спектральним складом відповідає приховуваному сигналу.

В наш час в основному застосовуються системи просторового зашумлення, які використовують перешкоди типу «білий шум», тобто випромінюють широкосмуговий шумовий сигнал (як правило, з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот), який істотно перевищує рівні побічних електромагнітних випромінювань. Такі системи застосовуються для захисту широкого класу технічних засобів: електронно-обчислювальної техніки, систем звукопідсилення і звукового супроводу, систем внутрішнього телебачення і т.ін.

Генератори шуму виконуються або у вигляді окремого блоку з живленням від мережі 220 В, або у вигляді окремої плати, що встановлюється (вбудовується) у вільний слот системного блоку комп'ютера з живленням від загальної шини комп'ютера.

Діапазон робочих частот генераторів шуму простягається від 0,01...0,1 до 1000 МГц. При потужності випромінювання близько 20 Вт забезпечується спектральна щільність перешкоди 40...80 дБ.

У системах просторового зашумлення в основному використовуються слабонаправлені рамкові жорсткі і гнучкі антени. Рамкові гнучкі антени виконуються зі звичайного дроту і розгортаються у двох-трьох площинах, що забезпечує формування перешкодного сигналу як з вертикальною, так і з горизонтальною поляризацією в усіх площинах.

При використанні систем просторового зашумлення необхідно пам’ятати, що поряд з перешкодами засобам розвідки створюються перешкоди і іншим радіоелектронним засобам (наприклад, систем телебачення, радіозв’язку тощо). Тому при введенні в експлуатацію системи просторового зашумлення необхідно проводити спеціальні дослідження за вимогами забезпечення електромагнітної сумісності (ЕМС). Крім того, рівні перешкод, що створюються системою зашумлення, повинні відповідати санітарно-гігієнічним нормам. Однак норми на рівні електромагнітних випромінювань за вимогами ЕМС істотно суворіше санітарно-гігієнічних норм. Отже, основну увагу необхідно приділяти безпосередньому виконанню норм ЕМС.

Просторове зашумлення ефективне не тільки для закриття електромагнітного, а й електричного каналів витоку інформації, так як перешкоджаючий сигнал при випромінюванні наводиться в сполучних лініях і сторонніх провідниках, що виходять за межі контрольованої зони.

Системи лінійного зашумлення застосовуються для маскування наведених небезпечних сигналів в сторонніх провідниках і сполучних лініях, що виходять за межі контрольованої зони. Вони використовуються в тому випадку, якщо не забезпечується необхідне рознесення цих провідників і ТЗПІ (тобто не виконується вимога щодо Зони № 1), проте при цьому забезпечується вимога по Зоні № 2 (тобто відстань від ТЗПІ до межі контрольованої зони більше, ніж Зона № 2). У найпростішому випадку система лінійного зашумлення являє собою генератор шумового сигналу, що формує шумову маскуючу напругу із заданими спектральними, часовими і енергетичними характеристиками, який гальванічно підключається в лінію зашумлення (сторонній провідник).

На практиці найбільш часто подібні системи використовуються для зашумлення ліній електроживлення (наприклад, ліній електроживлення освітлювальної та розеточної мереж).

5.3. Програмно-апаратні засоби інформаційної безпеки

5.3.1. Основи побудови програмно-апаратних засобів інформаційної безпеки

Поповнення парку комп'ютерів і розвиток об'єктів зв'язку та інформатизації протягом останніх років дозволяють відзначити неухильне зростання їх кількості, залежність економіки від впроваджених систем і мереж, країни, зміни методології їх захисту.

У цій сфері спостерігаються такі тенденції:

1. Розширення функціональних можливостей і здешевлення вартості комп'ютера;

2. Спеціалізація стаціонарних комп'ютерів в напрямках:

- домашнього та офісного застосування;
- функціонування в якості робочих станцій об'єктів зв'язку та інформатизації;
- функціонування в якості серверів у виробничих, транспортних, оборонних системах, у системах зв'язку тощо;
- функціонування в якості суперкомп'ютерів;

3. Підвищення попиту на комп'ютери із засобами захисту від НСД до інформації та засобами захисту від витоку інформації по каналах побічних електромагнітних випромінювань і наводок;

4. Інтеграція комп'ютерів із засобами зв'язку;

5. Удосконалення показників і характеристик як комп'ютерів, так і ПЗ.

Основні вимоги до технічних і програмних засобів (ТЗ і ПЗ) об'єктів зв'язку та інформатизації викладені в ряді нормативних документів.

Розробки та виробництва сучасних засобів захисту від НСД до інформації передувало виконання науково-дослідних робіт в цій галузі. Більшість розробників на початковому етапі були зосереджені на створенні тільки ПЗ, що реалізує функції захисту в

АС, що не може гарантувати надійного захисту АС від НСД до інформації.

Методологія застосування апаратного захисту, визнана необхідною основою побудови систем захисту від несанкціонованого доступу до інформації. Основні ідеї цього підходу полягають у наступному:

- комплексний підхід до вирішення питань інформаційної безпеки в АС від НСД;
- визнання мультиплікативної парадигми захисту, і, як наслідок, рівну увагу надійності реалізації контрольних процедур на всіх етапах роботи АС;
- «матеріалістичне» рішення «основного питання» інформаційної безпеки: «що первинне – hard або soft?»;
- послідовна відмова від програмних методів контролю як очевидно ненадійних і перенесення найбільш критичних контрольних процедур на апаратний рівень;
- максимально можливий поділ умовно-постійних і умовно-змінних елементів контрольних операцій;
- побудова засобів захисту інформації від несанкціонованого доступу (ЗЗІ НСД), максимально незалежних від операційних і файлових систем, що застосовуються в АС. Це виконання процедур ідентифікації/аутентифікації, контролю цілісності апаратних і програмних засобів АС до завантаження операційної системи, адміністрування і т.ін.

Основним об’єктом програмно-апаратного захисту інформаційних процесів та інформації є персональний комп’ютер, побутовій та іншій – корпоративна обчислювальна мережа підприємства, організації і фірми. Загрози можуть виходити від законного користувача (співробітника фірми) і порушника, який перебуває за межами організації і робочому місці.

5.3.2. Технічні засоби програмно-апаратного захисту інформації

Розглянемо реалізацію програмно-апаратного захисту інформації на прикладі продукції фірми Особливе конструкторське бюро систем автоматизованого проектування (ОКБ САПР).

Основою побудови систем захисту від несанкціонованого доступу ОКБ САПР є програмно-апаратний модуль довіреного завантаження (АМДЗ) – «Акорд-АМДЗ». Цей модуль забезпечує режим довіреного завантаження в різних операційних середовищах: MS DOS; Windows; OS/2; Unix; Linux.

Основним принципом роботи "Акорд-АМДЗ" є виконання процедур, що реалізують основні функції системи захисту інформації до завантаження ОС. Процедури ідентифікації /аутентифікації користувача, контролю цілісності апаратних і програмних засобів, адміністрування, блокування завантаження операційної системи з зовнішніх носіїв інформації розміщені у внутрішній пам'яті мікроконтролера плати «Акорд». Таким чином, користувач не має можливості зміни процедур, які впливають на функціональність системи захисту інформації. У незалежній пам'яті контролера «Акорд» зберігається інформація про персональні дані користувачів, дані для контролю цілісності програмних і апаратних засобів, журнал реєстрації та обліку системних подій і дій користувача.

Ці дані можуть бути змінені тільки авторизованим адміністратором безпеки інформації, так як доступ до незалежної пам'яті повністю визначається логікою роботи програмного забезпечення, розміщеного в мікроконтролері плати.

Засоби захисту інформації від несанкціонованого доступу сімейства «Акорд» реалізовані на базі контролера PCI мають свій ідентифікатор, наданий асоціацією розробників даних пристроїв (Vendor ID-1795).

Для організацій, що використовують промислові PC комп'ютери з шинним інтерфейсом PC/104 призначений програмно-апаратний комплекс «Аккорд-PC104». Він може застосовуватися в спеціалізованих комп'ютерах, використовуваних в бортовій апаратурі (наземні, повітряні, морські та промислові

системи), у вимірювальній апаратурі, у пристроях зв'язку, мобільних системах тощо.

У співпроцесорі безпеки «Аккорд-СБ» інтегровані всі необхідні засоби для реалізації комплексного захисту інформації від несанкціонованого доступу. Контролер співпроцесора безпеки «Акорд-СБ/2» має високопродуктивний мікропроцесор і апаратний прискорювач математичних функцій. Доступ до функцій цього процесора визначається вбудованим програмним забезпеченням контролера.

Використовуючи бібліотеку програмування контролера співпроцесора безпеки «Акорд-СБ/2» (SDK), розробник може застосовувати цей комплекс як багатофункціональний пристрій. Зокрема, окрім завдань із захисту інформації від несанкціонованого доступу, він може бути використаний для передавання конфіденційної інформації по відкритих каналах зв'язку в зашифрованому вигляді з високою швидкістю оброблення і передавання даних, шифрування дисків, формування та перевірки ЕЦП, захисту електронних документів з використанням захисних кодів аутентифікації (ЗКА), а також в якості брандмауера.

Вимоги до апаратних ЗЗІ та принципи апаратного захисту, реалізовані в ЗЗІ НСД сімейства «Акорд» застосовуються великими розробниками засобів захисту, які діють на українському ринку ЗЗІ. Застосування потужної апаратної підтримки в комплексах ЗЗІ НСД сімейства «Акорд» дозволило вийти на новий рівень у розвитку засобів захисту інформації. Як відомо для побудови автоматизованих систем за класами захищеності потрібна установка правил розмежування доступу до її інформаційних ресурсів.

Для реалізації функцій розмежування доступу користувачів до інформаційних ресурсів і створення ізольованого програмного середовища (ІПС) розроблено спеціальне програмне забезпечення, що підтримує всі типи контролерів «Акорд», включаючи роботу з датчиком випадкових чисел та реалізований мандатний принцип доступу суб'єктів до інформаційних ресурсів. Спеціальне ПЗ, що реалізує функції розмежування доступу, дозволяє адміністратору безпеки інформації описати будь-яку суперечливу політику безпеки на основі найбільш повного набору атрибутів (більше 15 атрибутів

з доступу до файлів і каталогів) і міток конфіденційності об'єктів (файлів) і процесів (програм), з допомогою яких здійснюється їх обробка.

Для повноцінного захисту локальної обчислювальної мережі пропонується комплексна технологія:

- установку на робочих станціях ЗЗІ «Акорд АМДЗ» з ПЗ «Аккорд»;
- установку підсистеми контролю цілісності на кожному файл-сервері;
- установку підсистеми розподіленого аудиту та управління;
- установку підсистеми посиленої аутентифікації.

Управління перерахованими вище підсистемами в ЛОМ забезпечується за допомогою автоматизованого робочого місця адміністратора безпеки (АРМ АБІ). Дана технологія дозволяє адміністратору безпеки інформації однозначно розпізнавати авторизованих користувачів і зареєстровані робочі станції в мережі; в режимі реального часу контролювати завдання, що виконуються користувачами; в разі несанкціонованих дій блокувати робочі станції, з яких такі дії здійснювалися; віддалено вести адміністрування. Особливий інтерес представляє підсистема посиленої аутентифікації, суть якої полягає в додатковому механізмі перевірки автентичності робочих станцій. Процедура перевірки автентичності виконується не тільки в момент підключення станції, але і з встановленою адміністратором періодичністю. Підсистема запобігає як підміні локальної станції або сервера, так і підключенню в ЛОМ нелегальних станцій/серверів. Посилена аутентифікація в ЛОМ заснована на застосуванні математичних методів, що дозволяють однозначно розпізнати учасників діалогу.

Як відомо, неможливо вирішити всі питання обробки інформації в АС тільки засобами захисту від несанкціонованого доступу до інформації, що захищається. Тому необхідно також забезпечити юридичну доказовість достовірності електронних документів.

Запропонований шлях подолання цієї проблеми – технологія захисту електронних документів з використанням захисних кодів

аутентифікації (ЗКА). Дана технологія вже використовується в банківських платіжних системах з метою запобігання спробам зловмисників ввести фіктивні або модифікувати оброблювані електронні банківські документи, а також з метою організації наскрізного контролю при проходженні електронних документів всіх призначених етапів їх існування (створення, оброблення, передавання, зберігання). Це забезпечується установкою на документ ЗКА. В результаті електронний документ на кожному етапі обробки має два ЗКА, перший з яких дозволяє авторизувати і проконтролювати його цілісність на попередньому етапі обробки, а другий – є його індивідуальною ознакою на поточному.

Технологічний захист електронного документообігу реалізується всіма типами контролерів сімейства «Акорд» та пристроями: блок установки кодів аутентифікації (БУКА); виріб «ШАПКА» (Шифрування Аутентифікація Підпис Коди Аутентифікації).

Виріб «ШАПКА» містить мікропроцесор з вбудованим програмним забезпеченням, апаратний датчик випадкових чисел і підключається через наявний інтерфейс – шину USB і може виконувати операції шифрування, гешування, формування і перевірку електронного цифрового підпису, формування і перевірку захисних кодів аутентифікації. У виробу є захищений електронний диск для запису інформації користувача.

Будь-яка система захисту інформації – це комплекс організаційно-технічних заходів, який включає в себе сукупність правових норм, організаційних заходів та програмно-технічних засобів захисту, спрямованих на протидію загрозам об’єкту захисту з метою зведення до мінімуму можливих збитків користувачів і власників системи. Без організаційних заходів, наявності чіткої організаційно-розпорядчої системи на об’єкті захисту інформації ефективність будь-яких технічних ЗЗІ знижується. Тому велике значення та увагу необхідно приділяти питанням розробки нормативно-технічної та методичної документації, комплектів організаційно-розпорядчих документів з політики захисту об’єктів захисту інформації відповідно до чинного законодавства.

Розділ II

РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ І ТЕХНОЛОГІЯХ

Тема 6. Основні програмно-технічні заходи рівня інформаційної безпеки в комп'ютерних системах і технологіях

6.1. Основні поняття програмно-технічного рівня інформаційної безпеки в комп'ютерних системах і технологіях

Програмно-технічні заходи, тобто заходи, спрямовані на контроль комп'ютерних сутностей – обладнання, програм і/або даних, утворюють останній і найважливіший рубіж інфобезпеки. Нагадаємо, що основну частину збитків завдають дії легальних користувачів, по відношенню до яких процедурні регулятори не можуть дати вирішального ефекту. Головні вороги – некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

Комп'ютери допомогли автоматизувати багато галузей людської діяльності. Цілком природним є бажання покласти на них і забезпечення власної безпеки. Навіть фізичний захист все частіше доручають інтегрованим КС, що дозволяє одночасно відстежувати переміщення співробітників і по простору організації, і по інформаційному простору. Це друга причина, яка пояснює важливість програмно-технічних заходів.

Слід, однак, враховувати, що швидкий розвиток ІТ не тільки дає нові можливості захисту, а й об'єктивно ускладнює забезпечення надійного захисту, якщо спиратися виключно на заходи програмно-технічного рівня.

Це обумовлено наступними причинами:

- підвищення швидкодії мікросхем, розвиток архітектур з високим ступенем паралелізму дозволяє методом грубої сили долати бар'єри (перш за все криптографічні), які раніше здавалися неприступними;
- розвиток мереж і мережевих технологій, збільшення числа зв'язків між інформаційними системами, зростання пропускної здатності каналів розширюють число зловмисників, що мають технічну можливість організовувати атаки;
- поява нових інформаційних сервісів веде і до появи нових вразливих місць як «всередині» сервісів, так і на їх стиках;
- конкуренція серед виробників програмного забезпечення змушує скорочувати терміни розробки, що веде до зниження якості тестування та випуску продуктів з дефектами захисту;
- нав'язувана споживачам парадигма постійного нарощування апаратного і програмного забезпечення не дозволяє довго залишатися в межах надійних, апробованих конфігурацій і, крім того, вступає в конфлікт з бюджетними обмеженнями, через що знижується частка асигнувань на безпеку.

Перераховані чинники зайвий раз підкреслюють важливість комплексного підходу до інформаційної безпеки, а також необхідність динамічної позиції при виборі і супроводі програмно-технічних регуляторів.

При такому підході центральним для програмно-технічного рівня є поняття сервісу безпеки.

Дотримуючись об'єктно-орієнтованого підходу, при розгляді інформаційної системи з одиничним рівнем деталізації ми побачимо сукупність наданих нею інформаційних сервісів. Назвемо їх основними. Щоб вони могли функціонувати і володіли необхідними властивостями, необхідно кілька рівнів додаткових (допоміжних) сервісів – від СУБД і моніторів транзакцій до ядра операційної системи і устаткування.

До допоміжних належать сервіси безпеки. Серед них нас насамперед будуть цікавити універсальні, високорівневі сервіси безпеки, що використовуються різними основними і допоміжними сервісами. Далі будуть наведені:

- ідентифікація та аутентифікація;
- управління доступом;
- протоколювання і аудит;
- шифрування;
- контроль цілісності;
- екранування;
- аналіз захищеності;
- забезпечення відмовостійкості;
- забезпечення безпечного відновлення;
- тунелювання;
- управління.

Будуть описані вимоги до сервісів безпеки, їх функціональність, можливі методи реалізації, місце в загальній архітектурі.

Якщо зіставити наведений перелік сервісів з класами функціональних вимог «Загальних критеріїв», то стає очевидною їхня істотна розбіжність. Ми відмовилися від розгляду питань, пов'язаних з приватними даними, з наступних причин. На наш погляд, сервіс безпеки, хоча б частково, повинен знаходитися в розпорядженні того, кого він захищає. У ситуації з приватними даними це не так: критично важливі компоненти зосереджені не на

клієнтській стороні, а на стороні сервера, так що приватність, по суті, виявляється властивістю запропонованої інформаційної послуги (в найпростішому випадку приватність досягається збереженням конфіденційності серверної реєстраційної інформації та захистом від перехоплення даних, для чого досить перерахованих вище сервісів безпеки).

З іншого боку, наведений перелік ширше, ніж у «Загальних умовах», оскільки в нього входять екранування, аналіз захищеності і тунелювання. Ми покажемо, що ці сервіси мають важливе самостійне значення і, крім того, можуть комбінуватися з іншими сервісами для отримання таких необхідних захисних засобів, як, наприклад, віртуальні власні мережі.

Сукупність перерахованих вище сервісів безпеки ми будемо називати повним набором. Відповідно до сучасних поглядів, він достатній для побудови надійного захисту на програмно-технічному рівні, при дотриманні цілого ряду додаткових умов (відсутність вразливостей, безпечне адміністрування і т.ін.).

Для проведення класифікації сервісів безпеки і визначення їх місця в загальній архітектурі доцільно поділити заходи безпеки на наступні види:

- превентивні, що перешкоджають порушенню ІБ;
- заходи виявлення порушень;
- локалізуючі, що звужують зону впливу порушень;
- заходи з вдстеження порушника;
- заходи відновлення режиму безпеки.

Більшість сервісів безпеки потрапляє в число превентивних, і це, безумовно, правильно. Аудит і контроль цілісності здатні допомогти у виявленні порушень. Активний аудит, крім того, дозволяє запрограмувати реакцію на порушення з метою локалізації та/або відстеження. Спрямованість сервісів відмовостійкості і безпечного відновлення очевидна. Нарешті, управління відіграє інфраструктурну роль, обслуговуючи всі аспекти ІС.

6.2. Особливості сучасних інформаційних систем, істотні з погляду безпеки

ІС типової сучасної організації є досить складним утворенням, побудованим у багаторівневій архітектурі клієнт/сервер, яка користуються численними зовнішніми сервісами і, в свою чергу, надає свої послуги назовні. Навіть порівняно невеликі магазини, що забезпечують розрахунок з покупцями з пластикових карт (і, звичайно, мають зовнішній Web-сервер), критичним чином залежать від своїх ІС і, зокрема (разом з покупцями), від захищеності всіх компонентів систем і комунікацій між ними.

З погляду безпеки найбільше істотними визнаються такі аспекти сучасних ІС:

- корпоративна мережа має кілька територіально рознесених частин (оскільки організація розташовується на кількох виробничих майданчиках), зв'язки між якими знаходяться у веденні зовнішнього постачальника послуг, виходячи за межі зони, контрольованої організацією;
- корпоративна мережа має одне або кілька підключень до Інтернет;
- на кожному з виробничих майданчиків можуть перебувати критично важливі сервери, доступу до яких потребують працівники, що базуються на інших майданчиках, мобільні працівники і, можливо, співробітники сторонніх організацій та інші зовнішні користувачі;
- для доступу користувачів можуть застосовуватися не тільки комп'ютери, але і споживчі пристрої, що використовують, зокрема, бездротовий зв'язок;
- протягом одного сеансу роботи користувачеві доводиться звертатися до декількох інформаційних сервісів, які спираються на різні апаратно-програмні платформи;
- до доступності інформаційних сервісів висуваються жорсткі вимоги, що зазвичай виражаються в необхідності цілодобового

функціонування з максимальним часом простою порядку хвилин або десятків хвилин;

• інформаційна система являє собою мережу з активними агентами, тобто в процесі роботи програмні компоненти, такі як аплети або сервлети, передаються з однієї машини на іншу і виконуються в цільовому середовищі, підтримуючи зв'язок з віддаленими компонентами;

• не всі призначені для користувача системи контролюються мережевими і/або системними адміністраторами організації;

• програмне забезпечення, особливо отримане по мережі, не може вважатися довіреним, в ньому можуть бути присутніми шкідливі елементи або помилки, що створюють вразливі місця у захисті;

• конфігурація інформаційної системи постійно змінюється на рівнях адміністративних даних, програм і апаратури (змінюється склад користувачів, їхні привілеї, версії програм, з'являються нові сервіси, нова апаратура тощо).

Слід враховувати ще принаймні два моменти. По-перше, для кожного сервісу основні грані ІБ (доступність, цілісність, конфіденційність) трактуються по-своєму. Цілісність з точки зору системи управління базами даних і з точки зору поштового сервера – речі принципово різні. Безглуздо говорити про безпеку локальної або іншої мережі взагалі, якщо мережа включає в себе різнорідні компоненти. Слід аналізувати захищеність сервісів, що функціонують в мережі. Для різних сервісів і захист будують по-різному. По-друге, основна загроза інформаційній безпеці організацій як і раніше іде не від зовнішніх зловмисників, а від власних співробітників, які з тієї чи іншої причини не є лояльними.

З огляду на викладені вище причини далі будуть розглядатися розподілені, різнорідні, багатосервісні, еволюціонуючі системи.

6.3. Архітектурна безпека

Сервіси безпеки, якими б потужними і стійкими вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки розумна, перевірена архітектура здатна зробити ефективним об'єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися і протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота і зручність використання.

Теоретичною основою вирішення проблеми архітектурної безпеки є фундаментальне положення «Помаранчевої книги» для мережевих конфігурацій, що складається з наступних тверджень:

а) кожен суб'єкт (тобто процес, який діє від імені будь-якого користувача) міститься всередині одного компонента і може здійснювати безпосередній доступ до об'єктів тільки в межах цього компонента;

б) кожен компонент містить свій монітор звернень, що відслідковує всі локальні спроби доступу, і всі монітори проводять в життя узгоджену політику безпеки;

в) комунікаційні канали, що зв'язують компоненти, зберігають конфіденційність і цілісність інформації, що передається;

г) сукупність всіх моніторів утворює єдиний монітор звернень для всієї мережевої конфігурації.

Звернемо увагу на три принципи, що містяться у наведеному положенні:

- необхідність вироблення і проведення в життя єдиної політики безпеки;
- необхідність забезпечення конфіденційності і цілісності при мережевих взаємодіях;
- необхідність формування складових сервісів за змістовним принципом, щоб кожен отриманий таким чином компонент мав повний набір захисних засобів і з зовнішньої точки зору представляв собою єдине ціле (не повинно бути інформаційних потоків, що йдуть до незахищених сервісів).

Якщо який-небудь (складений) сервіс не володіє повним набором захисних засобів (склад повного набору описаний вище),

необхідно залучення додаткових сервісів, які ми будемо називати екрануючими. Екрануючі сервіси встановлюються на шляхах доступу до недостатньо захищених елементів, а один такий сервіс може екранувати (захищати) як завгодно велике число елементів.

З практичної точки зору найбільш важливими є наступні принципи архітектурної безпеки:

- безперервність захисту в просторі і часі, неможливість оминути захисні засоби;
- слідування визнаним стандартам, використання апробованих рішень;
- ієрархічна організація ІС з невеликим числом сутностей на кожному рівні;
- посилення найслабшої ланки;
- неможливість переходу в небезпечний стан;
- мінімізація привілеїв;
- розподіл обов'язків;
- ешелонування оборони;
- різноманітність захисних засобів;
- простота і керованість інформаційної системи.

Пояснимо сенс перелічених принципів.

Якщо у зловмисника з'явиться можливість оминати захисні засоби, екрануючі сервіси повинні виключити подібну можливість.

Дотримання визнаних стандартів, використання апробованих рішень підвищує надійність ІС, зменшує ймовірність потрапляння в тупикову ситуацію, коли забезпечення безпеки вимагає непомірно великих затрат і принципових модифікацій.

Ієрархічна організація ІС з невеликим числом сутностей на кожному рівні необхідна з технологічних міркувань. При порушенні цього принципу система стане топологічно некерованою і, отже, забезпечити її безпеку буде неможливо.

Надійність будь-якої оборони визначається її найслабшою ланкою. Зловмисник не боротиметься проти сили, він віддасть перевагу легкій перемозі над слабкістю. Часто самою слабкою ланкою виявляється не комп'ютер або програма, а людина, і тоді проблема забезпечення інформаційної безпеки набуває нетехнічного характеру.

Принцип неможливості переходу в небезпечний стан означає, що при будь-яких обставинах, в тому числі позаштатних, захисний засіб або повністю виконує свої функції, або цілком блокує доступ. Образно кажучи, якщо фортеці механізм розвідного мосту ламається, міст повинен залишатися у піднятому стані, перешкоджаючи проходу ворога.

Принцип мінімізації привілеїв вимагає виділяти користувачам і адміністраторам тільки ті права доступу, які необхідні їм для виконання службових обов'язків. Призначення цього принципу – зменшити втрати від випадкових або навмисних некоректних дій користувачів і адміністраторів.

Принцип розподілу обов'язків передбачає такий розподіл ролей і відповідальності, щоб одна людина не могла порушити критично важливий для організації процес або створити пролом у захисті на замовлення зловмисників. Дотримання цього принципу особливо важливо, щоб запобігти зловмисним або некваліфікованим діям системного адміністратора.

Принцип ешелонування оборони вимагає не покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні розташовуватись програмно-технічні засоби, за ідентифікацією й аутентифікацією – керування доступом і, як останній рубіж, – протоколювання і аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання і аудит, істотно утрудняє непомітне виконання злочинних дій.

Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб потенційний зловмисник володів різноманітними і, по можливості, несумісними між собою навичками (наприклад, уміння долати високу огорожу і знання слабких місць декількох операційних систем).

Дуже важливий принцип простоти і керованості інформаційної системи в цілому і захисних засобів, особливо. Тільки для простого захисного засобу можна формально чи неформально довести його коректність. Тільки в простій і керованій системі можна перевірити узгодженість конфігурації різних компонентів і здійснити централізоване адміністрування. У

зв’язку з цим важливо відзначити інтегруючу роль Web-сервісу, що приховує розмаїття об’єктів і надає єдиний, наочний інтерфейс. Відповідно, якщо об’єкти деякого виду (наприклад, таблиці бази даних) доступні через Web, необхідно заблокувати прямий доступ до них, оскільки в іншому випадку система буде складною і погано керованою.

Для забезпечення високої доступності (безперервності функціонування) необхідно дотримуватися таких принципів архітектурної безпеки:

- Внесення в конфігурацію тієї чи іншої форми надмірності (резервне обладнання, запасні канали зв’язку тощо).
- Наявність засобів виявлення нештатних ситуацій.
- Наявність засобів реконфігурування для відновлення, ізоляції та/або заміни компонентів, які відмовили або піддалися атаці на доступність.
- Розосередження мережевого управління, відсутність єдиної точки відмови.
- Виділення підмереж і ізоляція груп користувачів один від одного. Дана міра, яка є узагальненням розподілу процесів на рівні операційної системи, обмежує зону ураження при можливих порушеннях інформаційної безпеки.

Ще одним важливим архітектурним принципом слід визнати мінімізацію обсягу захисних засобів, що виносяться на клієнтські системи.

Причин тому кілька:

- для доступу в корпоративну мережу можуть використовувати споживчі пристрої з обмеженою функціональністю;
- конфігурацію клієнтських систем важко або неможливо контролювати.

До необхідного мінімуму слід віднести реалізацію сервісів безпеки на мережевому і транспортному рівнях і підтримку механізмів аутентифікації, стійких до мережевих загроз.

Тема 7. Ідентифікація і аутентифікація, управління доступом

7.1. Ідентифікація та аутентифікація

7.1.1. Основні поняття ідентифікації і аутентифікації

Ідентифікація та аутентифікації застосовуються для обмеження доступу випадкових і незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси).

Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що засвідчує його особу, перевірити її справжність і потім надати (або не надати) цьому користувачеві можливість роботи з системою.

Наявність процедур аутентифікації і/або ідентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з поіменованими суб'єктами і об'єктами інформаційних систем.

Дамо визначення цих понять.

Ідентифікація – присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим.

Ідентифікація дозволяє суб'єкту (користувачеві, процесу, що діє від імені певного користувача, чи іншого апаратно-програмного компонента) назвати себе (повідомити своє ім'я). За допомогою аутентифікації інша сторона переконується, що суб'єкт дійсно той, за кого він себе видає.

Аутентифікація (встановлення автентичності) – перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора і підтвердження його автентичності. Іншими словами, аутентифікація полягає в перевірці: чи є суб'єкт, що підключається

тим, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка справжності».

Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність серверу) і двосторонньою (взаємною). Приклад односторонньої аутентифікації – процедура входу користувача в систему.

У мережевому середовищі, коли сторони ідентифікації /аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти:

- що слугує аутентифікатором (тобто використовується для підтвердження автентичності суб'єкта);
- як організований (і захищений) обмін даними ідентифікації/аутентифікації.

Тому при побудові систем ідентифікації і аутентифікації виникає проблема вибору зони, на основі якого здійснюються процедури ідентифікації і аутентифікації користувача. В якості ідентифікаторів зазвичай використовують:

- набір символів (пароль, секретний ключ, персональний ідентифікатор і т. ін.), який користувач запам'ятовує або для їх запам'ятовування використовує спеціальні засоби зберігання (електронні ключі);
- фізіологічні параметри людини (відбитки пальців, малюнок райдужної оболонки ока тощо) або особливості поведінки (особливості роботи на клавіатурі тощо).

За такого підходу суб'єкт може підтвердити свою автентичність, пред'явивши принаймні одну з наступних сутностей:

- щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ тощо);
- щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);
- щось, що є частина його самого (голос, відбитки пальців і т.ін., тобто свої біометричні характеристики).

Новітнім напрямком аутентифікації є доказ достовірності віддаленого користувача за його місцезнаходженням. Цей захисний механізм заснований на використанні системи космічної навігації, типу GPS (Global Positioning System). Користувач, що має апаратуру GPS, багаторазово посилає координати заданих супутників, що знаходяться в зоні прямої видимості. Підсистема аутентифікації, знаючи орбіти супутників, може з точністю до метра визначити місце розташування користувача. Висока надійність аутентифікації визначається тим, що орбіти супутників не завжди стабільні, передбачити які досить важко. Крім того, координати постійно змінюються, що виключає їх перехоплення. Такий метод аутентифікації може бути використаний у випадках, коли авторизований віддалений користувач повинен знаходитися в потрібному місці.

Загальна процедура ідентифікації і аутентифікації користувача при його доступі в захищену інформаційну систему полягає в наступному.

Користувач надає системі свій особистий ідентифікатор (наприклад, вводить пароль або надає палець для сканування відбитку). Далі система порівнює отриманий ідентифікатор з ідентифікаторами, що зберігаються в її базі. Якщо результат порівняння успішний, то користувач отримує доступ до системи в межах встановлених повноважень. У разі негативного результату система повідомляє про помилку і пропонує повторно ввести ідентифікатор. У тих випадках, коли користувач перевищує ліміт можливих повторів введення інформації (обмеження на кількість повторів є обов’язковою умовою для захищених систем) система тимчасово блокується і видається повідомлення про несанкціоновані дії (причому, може бути, і непомітно для користувача).

Якщо в процесі аутентифікації справжність суб’єкта встановлена, то система інформаційної безпеки повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю і розмежування доступу до ресурсів.

В цілому аутентифікація за рівнем інформаційної безпеки поділяється на три категорії:

1. Статична аутентифікація.
2. Стійка аутентифікація.
3. Постійна аутентифікація.

Перша категорія забезпечує захист тільки від несанкціонованих дій в системах, де порушник не може під час сеансу роботи прочитати аутентифікаційну інформацію. Прикладом засобів статичної аутентифікації є традиційні постійні паролі. Їх ефективність переважно залежить від складності вгадування паролів і, власне, від того, наскільки добре вони захищені.

Стійка аутентифікація використовує динамічні дані аутентифікації, що змінюються з кожним сеансом роботи. Реалізаціями стійкої аутентифікації є системи, що використовують одноразові паролі і електронні підписи. Стійка аутентифікація забезпечує захист від атак, де зловмисник може перехопити аутентифікаційну інформацію і використовувати її в наступних сеансах роботи.

Однак стійка аутентифікація не забезпечує захист від активних атак, в ході яких маскується зловмисник може оперативно (протягом сеансу аутентифікації) перехопити, модифікувати і вставити інформацію в потік переданих даних.

Постійна аутентифікація забезпечує ідентифікацію кожного блоку переданих даних, що оберігає їх від несанкціонованої модифікації або вставки. Прикладом реалізації зазначеної категорії аутентифікації є використання алгоритмів генерації електронних підписів для кожного біта інформації, що пересилається.

У відкритому мережевому середовищі між сторонами ідентифікації/аутентифікації не існує довіреного маршруту. Це означає, що в загальному випадку дані, передані суб’єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності. Необхідно забезпечити захист від пасивного і активного прослуховування мережі, тобто від перехоплення, зміни та/або відтворення даних. У цьому сенсі, передавання паролів у відкритому вигляді, очевидно, є незадовільним. Не рятує

становище і шифрування паролів, так як воно не захищає від відтворення, що обумовлює потребу у більш складних протоколах аутентифікації.

Надійна ідентифікація і аутентифікація утруднена не тільки через наявність мережевих загроз, а й по цілому ряду причин. По-перше, майже всі аутентифікаційні сутності можна дізнатися, вкрасти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача і системного адміністратора, з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже на його робоче місце може сісти інша людина), а це не тільки клопітно, але і підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб захисту, тим він дорожчий.

Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід в мережу – це, насамперед, вимога зручності для користувачів. Якщо в корпоративній мережі багато інфосервісів, що допускають незалежне звернення, то багаторазова ідентифікація/аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід в мережу став нормою. Домінуючі рішення у підході до вирішення цієї проблеми поки не сформувалися.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною і зручністю використання й адміністрування засобів ідентифікації і аутентифікації.

Цікаво відзначити, що сервіс ідентифікації/аутентифікації може стати об’єктом атак на доступність. Якщо система налаштована так, що після певного числа невдалих спроб пристрій введення ідентифікаційної інформації (такий, наприклад, як термінал) блокується, то зловмисник може зупинити роботу легального користувача буквально декількома натисканнями клавіш.

7.1.2. Парольна аутентифікація

Найбільш поширеними простими і звичними є методи аутентифікації, засновані на паролях – конфіденційних ідентифікаторах суб'єктів. В цьому випадку при введенні суб'єктом свого пароля підсистема аутентифікації порівнює його з паролем, що зберігаються в базі еталонних даних в зашифрованому вигляді. У разі збігу паролів підсистема аутентифікації дозволяє доступ до ресурсів системи.

Парольні методи аутентифікації за ступенем змінності паролів поділяються на:

- методи, які використовують постійні (багаторазово використовувані) паролі;
- методи, які використовують одноразові (що змінюються динамічно) паролі.

Використання одноразових або динамічних паролів є більш надійним методом парольного захисту.

Головна перевага парольної аутентифікації – простота і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, за сукупністю характеристик їх слід визнати найслабшим засобом перевірки автентичності.

Щоб не забути пароль, його достатньо часто роблять простим (ім'я подруги, назва спортивної команди тощо). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Відома класична історія про радянського розвідника Ріхарда Зорге, об'єкт уваги якого через слово говорив «карамба». Зрозуміло, цим же словом відкривався надсекретний сейф.

Іноді паролі з самого початку не зберігаються в таємниці, так як мають стандартні значення, зазначені в документації, і далеко не завжди після установки системи проводиться їх зміна.

Введення пароля можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на деякий час власника пароля. Теоретично в подібних випадках більш правильно задіяти засоби управління доступом, але на практиці так ніхто не чинить, а таємниця, яку знають двоє, це вже не таємниця.

Пароль можна вгадати «методом грубої сили», використовуючи, скажімо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна завантажити до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Проте заходи, що наведені нижче, дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не надто коротким, він повинен містити літери, цифри, знаки пунктуації тощо);
- управління терміном дії паролів, їх періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему (це утруднить застосування «методу грубої сили»);
- навчання користувачів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні і, отже, такі, які краще запам'ятовуються, паролі).

Перераховані заходи доцільно застосовувати завжди, навіть якщо поряд з паролями використовуються інші методи аутентифікації.

7.1.2.1. Одноразові паролі

Розглянуті вище паролі можна назвати багаторазовими; їх розкриття дозволяє зловмисникові діяти від імені легального користувача. Набагато більш потужним засобом, стійким до пасивного прослуховування мережі, є одноразові паролі.

Найбільш відомим програмним генератором одноразових паролів є система S/KEY компанії Bellcore. Ідея цієї системи полягає в наступному. Нехай є одностороння функція f (тобто функція, обчислити зворотну якої за прийнятний час не представляється можливим). Ця функція відома і користувачеві, і серверу аутентифікації. Нехай, далі, є секретний ключ K, відомий тільки користувачеві.

На етапі початкового адміністрування користувача функція f застосовується до ключа K n разів, після чого результат зберігається на сервері. Після цього процедура перевірки автентичності користувача виглядає наступним чином:

- сервер надсилає на призначену для користувача систему число (n-1);
- користувач застосовує функцію f до секретного ключа K (n-1) раз і відправляє результат по мережі на сервер аутентифікації;
- сервер застосовує функцію f до отриманого від користувача значенням і порівнює результат з раніше збереженою величиною. У разі збігу справжність користувача вважається встановленою, сервер запам’ятовує нове значення (надіслане користувачем) і зменшує на одиницю лічильник (n).

Насправді реалізація влаштована трохи складніше (окрім лічильника, сервер посилає початкове значення, яке використовується функцією (f), але для нас зараз це не важливо. Оскільки функція f незворотна, перехоплення пароля, так само як і отримання доступу до сервера аутентифікації, не дозволяють дізнатися секретний ключ K і передбачити наступний одноразовий пароль.

Система S/KEY має статус Internet-стандарту (RFC 1938).

Інший підхід до надійної аутентифікації складається в генерації нового пароля через невеликий проміжок часу (наприклад, кожні 60 секунд), для чого можуть використовуватися програми або спеціальні інтелектуальні карти (з практичної точки зору такі паролі можна вважати одноразовими). Серверу аутентифікації повинен бути відомий алгоритм генерації паролів і

асоційовані з ним параметри, окрім того, годинники клієнта і сервера повинні бути синхронізовані.

Останнім часом набули поширення комбіновані методи ідентифікації і аутентифікації, що вимагають, крім знання пароля, наявність картки (token) – спеціального пристрою, що підтверджує справжність суб'єкта.

Картки поділяють на два типи:

- пасивні (картки з пам'яттю);
- активні (інтелектуальні картки).

Найпоширенішими є пасивні картки з магнітною смугою, які зчитуються спеціальним пристроєм, що має клавіатуру і процесор. При використанні зазначеної картки користувач вводить свій ідентифікаційний номер. У разі його збігу з електронним варіантом, закодованим у картці, користувач отримує доступ до системи. Це дозволяє достовірно встановити особу, яка отримала доступ до системи і виключити несанкціоноване використання картки зловмисником (наприклад, при її втраті). Такий спосіб часто називають двокомпонентною аутентифікацією.

Інтелектуальні картки окрім пам'яті мають власний мікропроцесор. Це дозволяє реалізувати різні варіанти парольних методів захисту, наприклад, багаторазові паролі, динамічно мінливі паролі і інші.

7.1.2.2. Сервер аутентифікації Kerberos

Kerberos – це програмний продукт, розроблений в середині 1980-х років в Массачусетському технологічному інституті, що зазнав з того часу ряд принципових змін. Клієнтські компоненти Kerberos присутні в більшості сучасних операційних систем.

Kerberos призначений для вирішення наступного завдання. У відкритій (незахищеній) мережі, у вузлах зосереджені суб'єкти – користувачі, а також клієнтські і серверні програмні системи. Кожен суб'єкт мережі має секретний ключ. Щоб суб'єкт С міг довести свою справжність суб'єкту S (без цього S не буде

обслуговувати С), він повинен не тільки назвати себе, але і продемонструвати знання секретного ключа. С не може просто надіслати S свій секретний ключ, по-перше, тому, що мережа відкрита (доступна для пасивного і активного прослуховування), а, по-друге, тому, що S не знає (і не повинен знати) секретний ключ С. У цьому випадку потрібен менш прямолінійний спосіб показати знання секретного ключа.

Система Kerberos є довіреною третьою стороною (тобто стороною, якій довіряють всі), що володіє секретними ключами суб'єктів і допомагає їм в попарній перевірці автентичності.

Щоб за допомогою Kerberos отримати доступ до S (зазвичай це сервер), С (як правило – клієнт) посилає Kerberos запит, що містить відомості про нього (клієнта) і про запитувану послугу. У відповідь Kerberos повертає так званий квиток, зашифрований секретним ключем сервера, і копію частини інформації з квитка, зашифровану секретним ключем клієнта. Клієнт повинен розшифрувати другу порцію даних і переслати її разом з квитком сервера. Сервер, розшифрувавши квиток, може порівняти його вміст з додатковою інформацією, надісланою клієнтом.

Збіг свідчить про те, що клієнт зміг розшифрувати призначені йому дані (адже вміст квитка нікому, крім сервера і Kerberos, недоступний), тобто продемонстрував знання секретного ключа. Значить, клієнт – саме той, за кого себе видає. Підкреслимо, що секретні ключі в процесі перевірки справжності не передавалися по мережі (навіть у зашифрованому вигляді) – вони тільки використовувалися для шифрування.

Організація первинного обміну ключами між Kerberos і суб'єктами і те, як суб'єкти зберігають свої секретні ключі – питання окреме, але потрібно відзначити, що Kerberos не тільки стійкий до мережевих загроз, але і підтримує концепцію єдиного входу в мережу.

Проілюструємо описану процедуру (рис 7.1).

Тут c і s – відомості (наприклад, ім'я), відповідно, про клієнта і сервер, d1 і d2 – додаткова (по відношенню до квитка) інформація, Tc.s – квиток для клієнта С на обслуговування у сервера S, Kc і Ks –

секретні ключі клієнта і сервера, {info} K – інформація info, зашифрована ключем K.

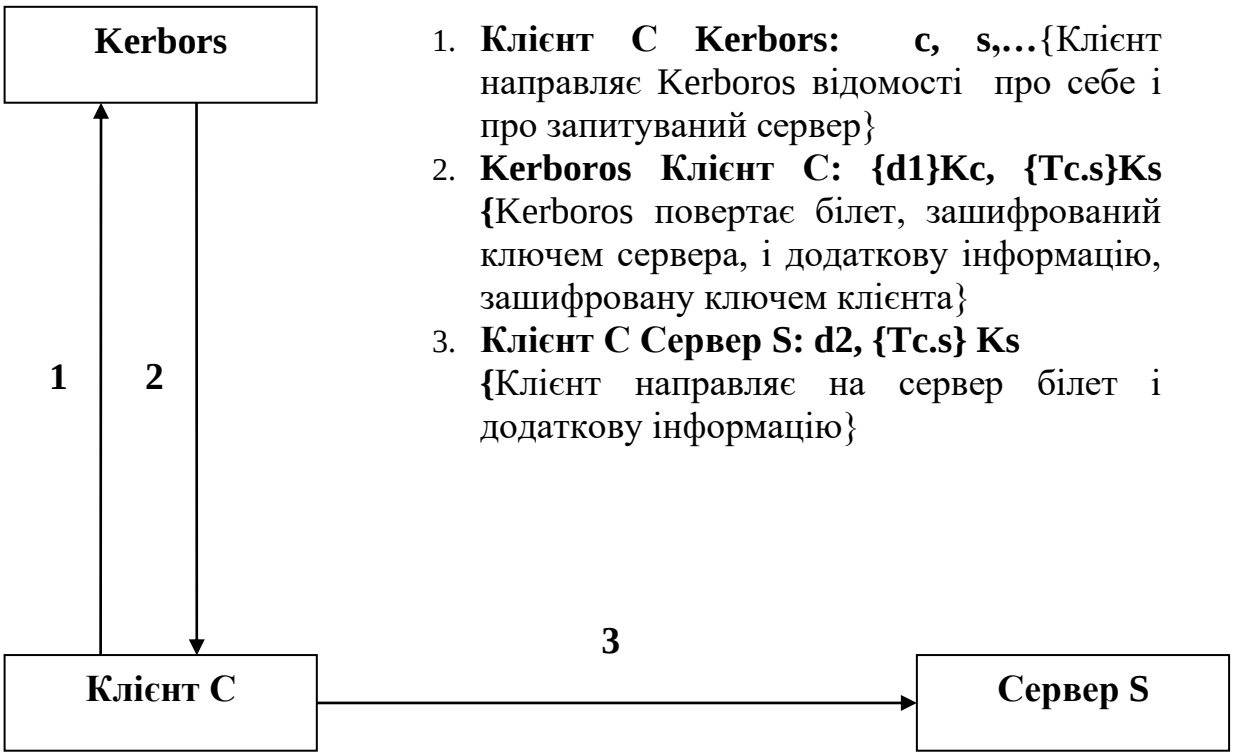


Рис. 7.1. Перевірка сервером S автентичності клієнта C

Необхідно відзначити, що наведена схема є спрощеною версією реальної процедури перевірки автентичності.

7.1.5. Ідентифікація/аутентифікація за допомогою біометричних даних

Методи аутентифікації, засновані на вимірюванні біометричних параметрів людини, забезпечують майже 100% ідентифікацію, вирішуючи проблеми втрати паролів і особистих ідентифікаторів. Однак ці методи не можна використовувати при ідентифікації процесів або даних (об’єктів даних), вони тільки розвиваються у цьому напрямку і вимагають досить складного обладнання.

Біометрія є сукупністю автоматизованих методів ідентифікації та/або аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. До фізіологічних характеристик належать особливості відбитків пальців, сітківки очей, геометрія руки та обличчя тощо; до поведінкових – динаміка підпису (ручного), стиль роботи з клавіатурою. На стику фізіології і поведінки знаходяться аналіз особливостей голосу і розпізнавання мови.

Біометрією у всьому світі займаються дуже давно, проте довгий час все, що було пов’язано з нею, відрізнялося складністю і дорожнечею. Останнім часом попит на біометричні продукти зростає, в першу чергу в зв’язку з розвитком електронної комерції. Це зрозуміло, оскільки з точки зору користувача набагато зручніше пред’явити себе самого, ніж щось запам’ятовувати. Попит народжує пропозицію, і на ринку з’явилися відносно недорогі апаратно-програмні продукти, орієнтовані в основному на розпізнавання відбитків пальців.

У загальному вигляді робота з біометричними даними організована таким чином. Спочатку створюється і підтримується база даних характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються, і результат обробки (біометричний шаблон) заноситься в базу даних (вихідні дані, такі як результат сканування пальця або сітківки, як правило, не зберігаються).

Надалі для ідентифікації (і одночасно аутентифікації) користувача процес зняття і обробки повторюється, після чого проводиться пошук в базі даних шаблонів. У разі успішного пошуку особистість користувача і її справжність вважаються встановленими. Для аутентифікації досить зробити порівняння з одним біометричних шаблоном, обраним на основі попередньо введених даних.

Зазвичай біометрію застосовують разом з іншими аутентифікатор, такими, наприклад, як інтелектуальні карти. Іноді біометрична аутентифікація є лише першим рубежем захисту і служить для активізації інтелектуальних карт, що зберігають

криптографічні секрети. У такому випадку біометричний шаблон зберігається на тій же карті.

Активність в галузі біометрії дуже велика. Організовано відповідний консорціум (див. http://www.biometrics.org), активно ведуться роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу тощо), публікується багато рекламних статей, в яких біометрія підноситься на рівень засобу забезпечення надбезпеки, що є доступною широким масам.

Але необхідно враховувати, що цей засіб має ті ж загрози, що і інші методи аутентифікації. По-перше, біометричний шаблон порівнюється ні з результатом первісної обробки характеристик користувача, а з тими, що прийшли до місця порівняння. А, як відомо, за час шляху багато чого може статися. По-друге, біометричні методи не більше надійні, ніж база даних шаблонів. По-третє, слід враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в «польових» умовах, коли, наприклад до пристрою сканування сітківки можуть піднести муляж тощо. По-четверте, біометричні дані людини змінюються, так що база шаблонів потребує супроводу, що створює певні проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка «пробоїна» для біометрії виявляється фатальною. Паролі, при всій їх ненадійності, можна змінити. Загублену аутентифікаційні карту можна анулювати і завести нову. Палець же, очі або голос змінити не можна. Якщо біометричні дані виявляться скомпрометованими, доведеться як мінімум проводити істотну модернізацію всієї системи.

7.2. Управління доступом

7.2.1. Основні поняття

Після виконання ідентифікації і аутентифікації підсистема захисту встановлює повноваження (сукупність прав) суб'єкта для подальшого контролю санкціонованого використання об'єктів інформаційної системи.

З традиційної точки зору засоби управління доступом дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі і процеси) можуть виконувати над об'єктами (інформацією та іншими комп'ютерними ресурсами). Зараз мова йде про логічне управлінні доступом, яке, на відміну від фізичного, реалізується ПЗ. Логічне управління доступом – це основний механізм багатокористувальницьких систем, покликаний забезпечити конфіденційність і цілісність об'єктів і, до певної міри, їх доступність (шляхом заборони обслуговування неавторизованих користувачів).

Зазвичай повноваження суб'єкта представляються: списком ресурсів, доступним користувачеві і правами доступу до кожного ресурсу зі списку.

Існують наступні методи розмежування доступу:

1. Розмежування доступу за списками.
2. Використання матриці встановлення повноважень.
3. Розмежування доступу за рівнями таємності і категоріям.
4. Парольне розмежування доступу.

При розмежуванні доступу за списками задаються відповідності: кожному користувачеві – список ресурсів і прав доступу до них або кожному ресурсу – список користувачів і їх прав доступу до цього ресурсу.

Списки дозволяють встановити права з точністю до користувача. Тут неважко додати права або явним чином заборонити доступ. Списки використовуються в підсистемах безпеки операційних систем і систем управління базами даних.

Приклад (операційна система Windows) розмежування доступу за списками для одного об’єкта показаний на рис. 7.2.

Списки доступу – виключно гнучкий засіб. З їх допомогою легко виконати вимогу про гранулярності прав з точністю до користувача. За допомогою списків нескладно додати права або явним чином заборонити доступ (наприклад, щоб покарати кількох членів групи користувачів). Безумовно, списки є найкращим засобом довільного управління доступом.

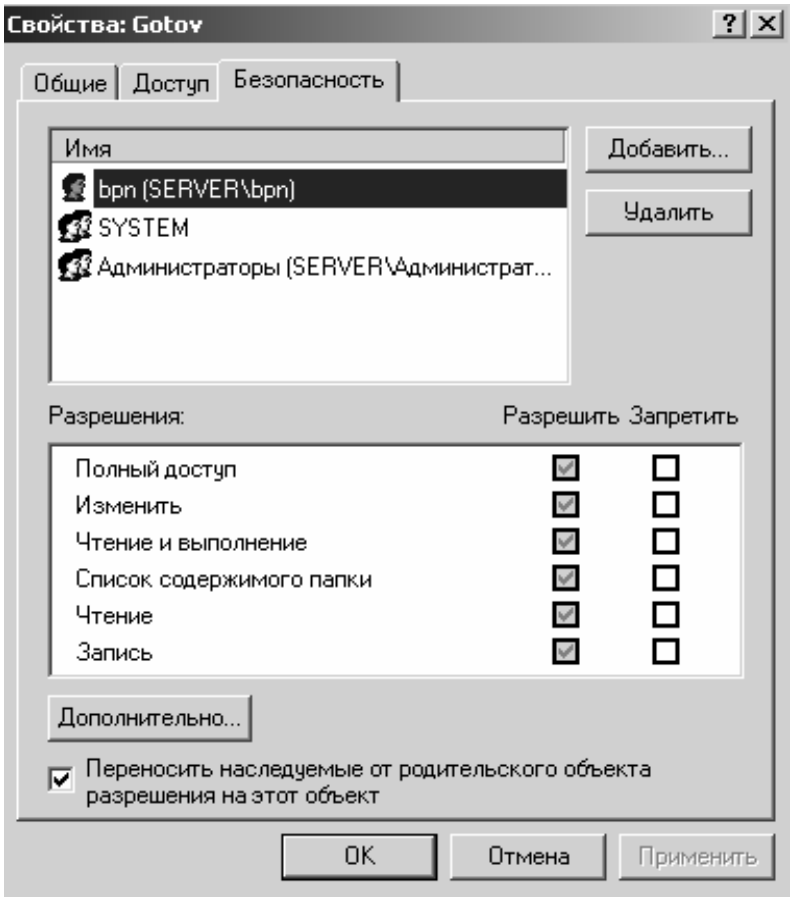


Рис. 7.2. Розмежування доступу за списками для одного об’єкта

Переважна більшість ОС і СУБД реалізують саме довільне керування доступом. Основна перевага довільного управління – гнучкість. Взагалі кажучи, для кожної пари «суб’єкт-об’єкт» можна незалежно задавати права доступу (особливо легко це робити, якщо використовуються списки управління доступом). На жаль, у «довільного» підходу є ряд недоліків.

Використання матриці встановлення повноважень має на увазі застосування матриці доступу (таблиці повноважень). У зазначеній матриці рядками є ідентифікатори суб'єктів, що мають доступ до інформаційної системи, а стовпцями – об'єкти (ресурси) інформаційної системи. Кожен елемент матриці може містити ім'я та розмір наданого ресурсу, право доступу (читання, запис та ін.), Посилання на іншу інформаційну структуру, що уточнює права доступу, посилання на програму, що управляє правами доступу тощо.

Розглянемо формальну постановку задачі в традиційному трактуванні. Нехай є сукупність суб'єктів і набір об'єктів. Завдання логічного управління доступом полягає в тому, щоб для кожної пари «суб'єкт-об'єкт» визначити множину допустимих операцій (залежну, можливо, від деяких додаткових умов) і контролювати виконання встановленого порядку.

Ставлення «суб'єкти-об'єкти» можна представити у вигляді матриці доступу, в рядках якої перераховані суб'єкти, у стовпцях – об'єкти, а в клітинах, розташованих на перетині рядків і стовпців, записані додаткові умови (наприклад, час і місце дії) і дозволені види доступу. Фрагмент матриці може виглядати, наприклад, так, як зображено у таблиці 7.1.

Табл. 7.1

Фрагмент матриці доступу

Суб'єкт	Диск C: \	Файл d: \ prog. exe	Принтер
Користувач 1	читання запис видалення	Виконання Видалення	Друк налаштування параметрів
Користувач 2	читання	Виконання	Друк з 9:00 до 17:00
Користувач 3	читання запис	Виконання	Друк з 17:00 до 9:00

Тема логічного управління доступом – одна з найскладніших у галузі ІБ. Справа в тому, що саме поняття об'єкта (а тим більше видів доступу) змінюється від сервісу до сервісу. Для операційної системи до об'єктів відносяться файли, пристрої та процеси. Стосовно файлів і пристроїв зазвичай розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення та додавання. Окремим правом може бути можливість передавання повноважень доступу іншим суб'єктам (так зване право володіння). Процеси можна створювати і знищувати. Сучасні операційні системи можуть підтримувати і інші об'єкти.

Для СУБД об'єкт – це база даних, таблиця, збережена процедура. У таблицях застосовуються операції пошуку, додавання, модифікації і видалення даних, у інших об'єктів інші види доступу.

Різноманітність об'єктів і застосовних до них операцій призводить до принципової децентралізації логічного управління доступом. Кожен сервіс повинен сам вирішувати, чи дозволити конкретному суб'єкта ту чи іншу операцію. Теоретично це узгоджується з сучасним об'єктно-орієнтованим підходом, на практиці ж призводить до значних труднощів.

Головна проблема полягає в тому, що до багатьох об'єктів можна отримати доступ за допомогою різних сервісів (можливо, при цьому доведеться подолати деякі технічні труднощі). Так, до реляційних таблиць можна дістатися не тільки засобами СУБД, але і шляхом безпосереднього читання файлів або дискових розділів, що підтримуються операційною системою (розібравшись попередньо в структурі зберігання об'єктів бази даних). В результаті при завданні матриці доступу потрібно брати до уваги не тільки принцип розподілу привілеїв для кожного сервісу, але і існуючі зв'язки між сервісами (доводиться дбати про узгодженість різних частин матриці).

Аналогічні труднощі виникають при експорті/імпорті даних, коли інформація про права доступу, як правило, втрачається (оскільки на новому сервісі вона не має сенсу). Отже, обмін даними між різними сервісами представляє особливу небезпеку з точки

зору управління доступом, а при проектуванні і реалізації різнорідної конфігурації необхідно подбати про узгоджений розподіл прав доступу суб'єктів до об'єктів і про мінімізацію числа способів експорту/імпорту даних.

При прийнятті рішення про надання доступу зазвичай аналізується наступна інформація:

- ідентифікатор суб'єкта (код користувача, мережева адреса комп'ютера тощо). Подібні ідентифікатори є основою довільного (або дискреційного) управління доступом;
- атрибути суб'єкта (мітка безпеки, група користувача тощо). Мітки безпеки – основа примусового (мандатного) управління доступом.

Матрицю доступу, з огляду на її розрідженість (більшість клітин – порожні), нерозумно зберігати у вигляді двомірного масиву. Зазвичай її зберігають за стовпцями, тобто для кожного об'єкта підтримується список «допущених» суб'єктів разом з їх правами. Елементами списків можуть бути імена груп і шаблони суб'єктів, що служить великою підмогою адміністратору. Деякі проблеми виникають тільки при видаленні суб'єкта, коли доводиться видаляти його ім'я з усіх списків доступу, але ця операція проводиться доволі нечасто.

Розосередження управління доступом веде до того, що довіреними повинні бути багато користувачів, а не тільки системні оператори або адміністратори. Через неуважність або некомпетентність співробітника, який володіє секретною інформацією, про цю інформацію можуть дізнатися і всі інші користувачі. Отже, довільність управління повинна бути доповнена жорстким контролем за реалізацією обраної політики безпеки.

Інший недолік, який є головним, полягає в тому, що права доступу існують окремо від даних. Ніщо не заважає користувачеві, що має доступ до секретної інформації, записати її в доступний всім файл або замінити корисну утиліту її «троянським» аналогом. Подібна «розділеність» прав і даних істотно ускладнює проведення декількома системами узгодженої політики безпеки і, головне, робить практично неможливим ефективний контроль узгодженості.

Повертаючись до питання подання матриці доступу, вкажемо, що для цього можна використовувати також функціональний спосіб, коли матрицю не зберігають в явному вигляді, а кожен раз обчислюють вміст відповідних клітин. Наприклад, при примусовому управлінні доступом застосовується порівняння міток безпеки суб'єкта та об'єкта.

Зручною надбудовою над засобами логічного управління доступом є обмежуючий інтерфейс, коли користувача позбавляють самої можливості спробувати зробити несанкціоновані дії, включивши в число видимих йому об'єктів тільки ті, до яких він має доступ. Подібний підхід зазвичай реалізують в межах системи меню (користувачеві показують лише допустимі варіанти вибору) або за допомогою обмежуючих оболонок, таких як restricted shell в ОС Unix.

Підкреслимо важливість управління доступом не тільки на рівні операційної системи, але і в межах інших сервісів, що входять до складу сучасних додатків, а також, наскільки це можливо, на «стиках» між сервісами. Тут на перший план виходить існування єдиної політики безпеки організації, а також кваліфіковане і узгоджене системне адміністрування.

Розмежування доступу за рівнями таємності і категоріям полягає в розподілі ресурсів інформаційної системи за рівнями таємності і категоріям.

При розмежуванні за ступенем секретності виділяють кілька рівнів, наприклад: загальний доступ, конфіденційно, таємно, цілком таємно. Повноваження кожного користувача задаються відповідно до максимальним рівнем секретності, до якого він допущений. Користувач має доступ до всіх даних, які мають рівень (гриф) секретності не вище, ніж йому визначено, наприклад, користувач має доступ до даних «секретно», також має доступ до даних «конфіденційно» і «загальний доступ».

При розмежування за категоріями задається і контролюється ранг категорії користувачів. Відповідно, всі ресурси інформаційної системи розподіляються за рівнями важливості, причому певному рівню відповідає категорія користувачів. Як приклад, де

використовуються категорії користувачів, наведемо операційну систему Windows, підсистема безпеки якої за замовчуванням підтримує наступні категорії (групи) користувачів: «адміністратор», «досвідчений користувач», «користувач» і «гість». Кожна з категорій має певний набір прав. Застосування категорій користувачів дозволяє спростити процедури призначення прав користувачів за рахунок застосування групових політик безпеки.

Парольне розмежування, представляє використання методів доступу суб'єктів до об'єктів по паролю. При цьому використовуються всі методи парольного захисту. Очевидно, що постійне використання паролів створює незручності користувачам і часові затримки. Тому зазначені методи використовують у виняткових ситуаціях.

На практиці зазвичай поєднують різні методи розмежування доступу. Наприклад, перші три методи посилюють парольним захистом.

Розмежування прав доступу є обов'язковим елементом захищеної ІС. Нагадаємо, що ще в «Помаранчевій книзі США» були введені поняття:

- довільне керування доступом;
- примусове управління доступом.

У ГОСТ Р 50739-95 «Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації» та в галузевих документах визначено два види (принципу) розмежування доступу:

- дискретне управління доступом;
- мандатне управління доступом.

Дискретне управління доступом являє собою розмежування доступу між поіменованими суб'єктами і поіменованими об'єктами. Суб'єкт з певним правом доступу може передати це право для будь-якого іншого суб'єкта. Цей вид організовується на базі методів розмежування за списками або за допомогою матриці.

Мандатне управління доступом засноване на зіставленні міток конфіденційності інформації, що міститься в об'єктах (файли,

папки, рисунки) і офіційного дозволу (допуску) суб'єкта до інформації відповідного рівня конфіденційності.

При уважному розгляді можна помітити, що дискретне управління доступом є ніщо інше, як довільне керування доступом (за «Помаранчевою книгою США»), а мандатне управління реалізує примусове управління доступом.

7.2.2. Рольове управління доступом

За великої кількості користувачів традиційні підсистеми управління доступом стають вкрай складними для адміністрування. Число зв'язків в них пропорційно добутку кількості користувачів на кількість об'єктів. Необхідні рішення в об'єктно-орієнтованому стилі, здатні цю складність знизити.

Таким рішенням є рольове управління доступом (РУД). Суть його в тому, що між користувачами і їх привілеями з'являються проміжні сутності – ролі. Для кожного користувача одночасно можуть бути активними кілька ролей, кожна з яких дає йому певні права (рис. 7.3).

Рольовий доступ нейтральний по відношенню до конкретних видів прав і способів їх перевірки. Його можна розглядати як об'єктно-орієнтований каркас, який полегшує адміністрування, оскільки він дозволяє зробити підсистему розмежування доступу керованої при як завгодно великому числі користувачів, перш за все за рахунок встановлення між ролями зв'язків, аналогічних спадкоємності в об'єктно-орієнтованих системах. Крім того, ролей має бути значно менше, ніж користувачів. В результаті кількість зв'язків, що адмініструються, стає пропорційним сумі (а не добутку) кількості користувачів і об'єктів, тобто величини, яку зменшити уже неможливо.

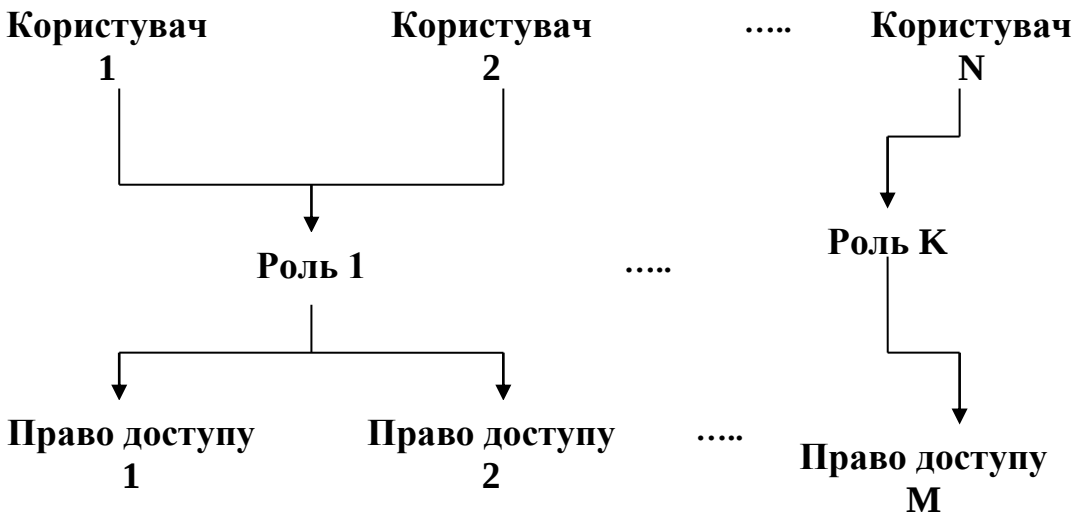


Рис. 7.3. Користувачі, об'єкти і ролі

Рольовий доступ розвивається більш 15 років (сама ідея ролей, зрозуміло, значно старша) як на рівні операційних систем, так і в межах СУБД та інших інформаційних сервісів. Зокрема, існують реалізації рольового доступу для Web-серверів.

У 2001 році Національний інститут стандартів і технологій США запропонував проект стандарту рольового управління доступом (див. http://csrc.nist.gov/rbac/), основні положення якого ми і розглянемо.

Рольове управління доступом оперує такими основними поняттями:

- користувач (людина, інтелектуальний автономний агент і т.ін.);
- сеанс роботи користувача;
- роль (зазвичай визначається відповідно до організаційної структури);
- об'єкт (сутність, доступ до якої розмежовується; наприклад, файл ОС або таблиця СУБД);
- операція (залежить від об'єкта: для файлів ОС – читання, запис, виконання тощо; для таблиць СУБД – вставка, видалення

тощо; для прикладних об’єктів операції можуть бути більш складними);

- право доступу (дозвіл виконувати певні операції над певними об’єктами).

Ролям приписуються користувачі і права доступу. Можна вважати, що вони (ролі) іменують відношення «багато до багатьох» між користувачами і правами. Ролі можуть бути приписані багатьом користувачам; один користувач може бути приписаний кільком ролям. Під час сеансу роботи користувача активізується підмножина ролей, яким він приписаний, в результаті чого він стає володарем об’єднання прав, приписаних активним ролям. Одночасно користувач може відкрити кілька сеансів.

Між ролями може бути визначено відношення часткового порядку, що називається спадкуванням. Якщо роль r_2 є спадкоємницею r_1, то всі права r_1 приписуються r_2, а всі користувачі r_2 приписуються r_1. Очевидно, що спадкування ролей відповідає спадкуванню класів в об’єктно-орієнтованому програмуванні, тільки праву доступу відповідають методи класів, а користувачам – об’єкти (екземпляри) класів.

Відношення спадкування є ієрархічним, причому права доступу і користувачі поширюються за рівнями ієрархії назустріч один одному. У загальному випадку спадкування є множинним, тобто у однієї ролі може бути кілька попередниць (і, природно, кілька спадкоємниць, яких ми будемо називати також наступницями).

Можна уявити собі формування ієрархії ролей, починаючи з мінімуму прав (і максимуму користувачів), що приписуються ролі «співробітник», з поступовим уточненням складу користувачів і додаванням прав (ролі «системний адміністратор», «бухгалтер» тощо), аж до ролі «керівник» (що не означає, що керівнику надаються необмежені права; як і іншим ролям, відповідно до принципу мінімізації привілеїв, цій ролі доцільно дозволити тільки те, що необхідно для виконання службових обов’язків). Фрагмент подібної ієрархії ролей показаний на рис. 7.4.

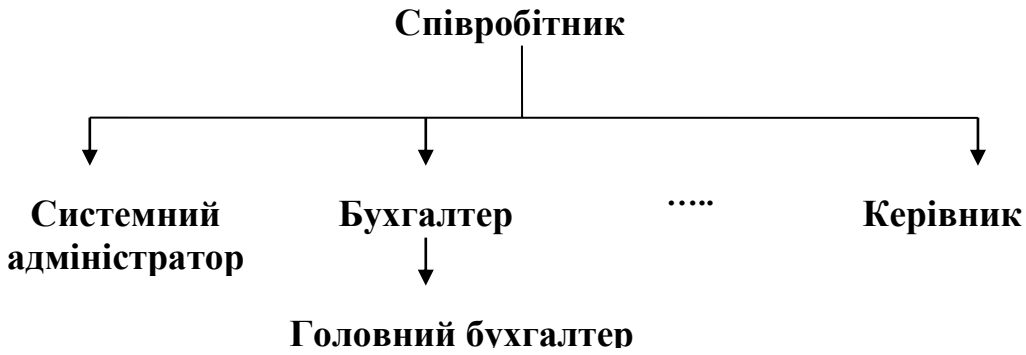


Рис. 7.4. Фрагмент ієрархії ролей

Для реалізації ще одного важливого принципу ІБ вводиться поняття розподілу обов'язків, причому в двох видах: статичному і динамічному.

Статичний розподіл обов'язків накладає обмеження на приписування користувачів ролям. У найпростішому випадку членство у деякій ролі забороняє приписування користувачу певної множини інших ролей. У загальному випадку це обмеження задається як пара «множина ролей – число» (де множина складається, принаймні, з двох ролей, а число повинно бути більше 1), так що ніякий користувач не може бути приписаний вказаному (або більшому) числу ролей із заданої множини. Наприклад, може існувати п'ять бухгалтерських ролей, але політика безпеки допускає членство не більше ніж у двох таких ролях (тут число = 3).

При наявності успадкування ролей обмеження набуває дещо складнішого вигляду, але суть залишається простою: при перевірці членства в ролях потрібно враховувати приписування користувачів ролям-спадкоємицям.

Динамічний розподіл обов'язків відрізняється від статичного тільки тим, що розглядаються ролі, одночасно активні (можливо, в різних сеансах) для даного користувача (а не ті, яким користувач статично приписаний). Наприклад, один користувач може грати роль і касира, і контролера, але не одночасно; щоб стати контролером, він повинен спочатку закрити касу. Тим самим

реалізується так зване часове обмеження довіри, що є аспектом мінімізації привілеїв.

Розглянутий стандарт містить специфікації трьох категорій функцій, необхідних для адміністрування:

1. Адміністративні функції (створення і супровід ролей і інших атрибутів рольового доступу): створити/видалити роль/користувача, приписати користувача/право участі або ліквідувати існуючу асоціацію, створити/видалити відношення успадкування між існуючими ролями, створити нову роль і зробити її спадкоємицею/попередницею існуючої ролі, створити/видалити обмеження для статичного/динамічного розподілу обов'язків.

2. Допоміжні функції (обслуговування сеансів роботи користувачів): відкрити сеанс роботи користувача з активацією набору ролей; активувати нову роль, деактивувати роль; перевірити правомірність доступу.

3. Інформаційні функції (отримання відомостей про поточну конфігурацію з урахуванням відношення спадкування). Тут проводиться розподіл на обов'язкові та необов'язкові функції. До числа перших належать отримання списку користувачів, приписаних ролі, і списку ролей, яким приписаний користувач.

Всі інші функції віднесені до розряду необов'язкових. Це отримання інформації про права, що приписані ролі; про права заданого користувача (якими він володіє як член множини ролей); про активні в цей момент сеансу ролі і права, про операції, які роль/користувач можуть здійснити над заданим об'єктом; про статичний/динамічний розподіл обов'язків.

Запропонований стандарт допомагає сформувати єдину термінологію і, що більш важливо, дозволяє оцінювати продукти з єдиних позицій, за єдиною шкалою.

7.2.3. Управління доступом в Java-середовищі

Java – це об'єктно-орієнтована система програмування, тому і управління доступом у ній спроектовано і реалізовано в об'єктному

стилі. З цієї причини розглянути Java-середовище для нас дуже важливо.

Перш за все, зупинимося на еволюції моделі безпеки Java. В JDK 1.0 була запропонована концепція «пісочниці» (sandbox) – замкнутого середовища, в якому виконуються потенційно ненадійні програми (аплети, що надійшли по мережі). Програми, які містяться на локальному комп'ютері, вважалися абсолютно надійними, і їм було доступно все, що доступно віртуальній Java-машині.

До обмежень, що накладаються «пісочницею», належить заборона на доступ до локальної файлової системи, на мережеву взаємодію з усіма хостами, крім джерела аплету тощо. Незалежно від рівня безпеки, що досягається при цьому (а проблеми виникали і з розподілом свій/чужий, і з визначенням джерела аплету), накладені обмеження слід визнати занадто обтяжливими: можливості для змістовних дій у аплетів майже не залишається.

Щоб впоратися з цією проблемою, в JDK 1.1 ввели розподіл джерел (точніше, розповсюджувачів) аплетів на надійні і ненадійні (джерело визначався за електронним підписом). Надійні аплети прирівнювалися в правах до «рідного» коду. Зроблене послаблення вирішило проблеми тих, кому прав не вистачало, але захист залишилася неешелонованим і, отже, неповним.

В JDK 1.2 сформувалася модель безпеки, яка використовується і в Java 2. Від моделі «пісочниці» відмовилися. Сформувалися три основних поняття: джерело програми; право і множина прав; політика безпеки.

Джерело програми визначається парою (URL, розповсюджувачі програми). Останні задаються набором цифрових сертифікатів.

Право – це абстрактне поняття, за яким, як і належить в об'єктному середовищі, стоять класи і об'єкти. У більшості випадків право визначається двома ланцюжками символів – ім'ям ресурсу і дією. Наприклад, в якості ресурсу може виступати файл, а в якості дії – читання. Найважливішим методом «правових»

об’єктів є implies (). Він перевіряє, чи слідує одне право (запитуване) з іншого (наявного).

Політика безпеки задає відповідність між джерелом і правами програм, що надійшли з нього (формально можна вважати, що кожному джерелу відповідає своя «пісочниця»). В JDK 1.2 «рідні» програми не мають будь-яких привілеїв у плані безпеки, і політика по відношенню до них може бути будь-якою. В результаті вийшов традиційний для сучасних ОС і СУБД механізм прав доступу з такими особливостями:

- Java-програми виступають не від імені користувача, що їх запустив, а від імені джерела програми;
- немає поняття власника ресурсів, який міг би змінювати права; останні задаються виключно політикою безпеки (формально можна вважати, що власником усього є той, хто формує політику);
- механізми безпеки забезпечені об’єктною обгорткою.

Дуже важливим поняттям в моделі безпеки JDK 1.2 є контекст виконання. Коли віртуальна Java-машина перевіряє права доступу об’єкта до системного ресурсу, вона розглядає не тільки поточний об’єкт, але і попередні елементи стека викликів. Доступ надається тільки тоді, коли потрібним правом володіють всі об’єкти в стеку. Розробники Java називають це реалізацією принципу мінімізації привілеїв.

На перший погляд, врахування контексту представляється логічним. Не можна допускати, щоб виклик будь-якого методу розширював права доступу хоча б з тієї причини, що доступ до системних ресурсів здійснюється не безпосередньо, а за допомогою системних об’єктів, що мають всі права.

На жаль, подібні доводи суперечать одному з основних принципів об’єктного підходу – принципу інкапсуляції. Якщо об’єкт А звертається до об’єкта В, він не може і не повинен знати, як реалізований В і якими ресурсами він користується для своїх цілей. Якщо А має право викликати будь-який метод В з деякими значеннями аргументів, В зобов’язаний обслужити виклик. В іншому випадку при формуванні політики безпеки доведеться

враховувати можливий граф викликів об’єктів, що, звичайно ж, неможливо.

Розробники Java усвідомлювали цю проблему. Щоб впоратися з нею, вони ввели поняття привілейованого інтервалу програми. При виконанні такого інтервалу контекст ігнорується. Привілейована програма відповідає за себе, не цікавлячись передісторією. Аналогом привілейованих програм є файли з бітами перевстановлення ідентифікатора користувача/групи в ОС Unix, що зайвий раз підтверджує традиційність підходу, реалізованого в JDK 1.2. Відомі загрози безпеки, які привносять подібні файли. Тепер це не найкращий засіб ОС Unix перекочував у Java.

В цілому засоби управління доступом в JDK 1.2 можна оцінити як «наполовину об’єктні». Реалізація оформлена у вигляді інтерфейсів і класів, проте як і раніше розмежовується доступ до необ’єктних сутностей – ресурсів у традиційному розумінні. Не враховується семантика доступу. Мають місце і інші зазначені вище концептуальні проблеми.

Можливий підхід до управління доступом в розподіленому об’єктному середовищі

Звісно ж, що в даний час проблема управління доступом існує в трьох майже не пов’язаних між собою проявах:

- традиційні моделі (дискреційна і мандатна);
- модель «пісочниця» (запропонована для Java-середовища і близькою їй системи Safe-Tcl);
- модель фільтрації (використовується в міжмережевих екранах).

На наш погляд, необхідно об’єднати існуючі підходи на основі їх розвитку та узагальнення.

Формальна постановка задачі розмежування доступу може виглядати наступним чином.

Розглядається множина об’єктів (у сенсі об’єктно-орієнтованого програмування). Частина об’єктів може бути контейнерами, групуються об’єкти-компоненти, які задають для них загальний контекст та виконують загальні функції і реалізують

перебір компонентів. Контейнери або вкладені один в один, або не мають загальних компонентів.

З кожним об'єктом асоційований набір інтерфейсів, забезпечених дескрипторами (ДІ). До об'єкту можна звернутися тільки за допомогою ДІ. Різні інтерфейси можуть надавати різні методи і бути доступними для різних об'єктів.

Кожен контейнер дозволяє опитати набір ДІ об'єктів-компонентів, які відповідають деякій умові. Результат, що повертається, у загальному випадку залежить від викликаючого об'єкта.

Об'єкти ізольовані один від одного. Єдиним видом міжоб'єктної взаємодії є виклик методу.

Передбачається, що використовуються надійні засоби аутентифікації та захисту комунікацій. У плані розмежування доступу локальні і віддалені виклики не розрізняються.

Передбачається також, що дозвіл або заборона на доступ не залежать від можливого паралельного виконання методів (синхронізація представляє окрему проблему, яка тут не розглядається).

Розмежовується доступ до інтерфейсів об'єктів, а також до методів об'єктів (з урахуванням значень фактичних параметрів виклику). Правила розмежування доступу (ПРД) задаються у вигляді предикатів над об'єктами.

Розглядається задача розмежування доступу для виділеного контейнера, компонентами якого повинні бути ті що викликаються і/або ті що викликають об'єкти. ДІ цього контейнера приймається загальновідомим. Вважається також, що між зовнішніми по відношенню до виділеного контейнера об'єктами можливі будь-які виклики.

Виконання ПРД контролюється монітором звернень.

При виклику методу ми будемо розділяти дії, що здійснюються викликаючим об'єктом (ініціація виклику) і методом, який викликається (прийом і завершення виклику).

При ініціації виклику може проводитися перетворення ДІ фактичних параметрів до вигляду, доступному викликаючого

методу («трансляція інтерфейсу»). Трансляція може мати місце, якщо об’єкт, що викликається не входить в той же контейнер, що і викликаючий.

Параметри методів можуть бути вхідними і/або вихідними. При прийомі виклику виникає інформаційний потік з вхідних параметрів у об’єкті виклику. У момент завершення виклику виникає інформаційний потік з викликаючого об’єкта у вихідні параметри. Ці потоки можуть фігурувати в правилах розмежування доступу.

Структуруємо множину всіх ПРД, виділивши чотири групи правил:

- політика безпеки контейнера;
- обмеження на метод, що викликається;
- обмеження на викликаючий метод;
- обмеження, що накладаються добровільно.

Правила, загальні для всіх об’єктів, що входять в контейнер С, назвемо політикою безпеки даного контейнера.

Нехай метод M_1 об’єкта O_1 в точці P_1 свого виконання повинен викликати метод М об’єкта О. Правила, яким повинен задовольняти М, можна розділити на три наступні підгрупи:

- правила, що описують вимоги до формальних параметрів виклику;
- правила, що описують вимоги до семантики М;
- реалізаційні правила, що накладають обмеження на можливі реалізації М;
- правила, що накладають обмеження на об’єкт виклику О.

Метод М об’єкта О, потенційно доступний для виклику, може пред’являти до викликаючого об’єкта наступні групи вимог:

- правила, що описують вимоги до фактичних параметрів виклику;
- правила, що накладають обмеження на викликаючий об’єкт.

Можна виділити три різновиди предикатів, що відповідають семантиці і/або особливостям реалізації методів:

- твердження про фактичні параметри виклику методу M в точці P_1;
- предикат, що описує семантику методу M;
- предикат, що описує особливості реалізації методу M.

Перераховані обмеження можна назвати добровільними, оскільки вони відповідають реальній поведінці об’єктів і не пов’язані з будь-якими зовнішніми вимогами.

Запропонована постановка задачі розмежування доступу відповідає сучасному етапу розвитку програмування, вона дозволяє побудувати як завгодно складну безпекову політику, знайти баланс між багатством виразних можливостей і ефективністю роботи монітора звернень.

Тема 8.1. Протоколювання і аудит, шифрування, контроль цілісності

8.1.1. Основні поняття протоколювання і аудиту

Реєстрація (протоколювання) є ще одним механізмом забезпечення захищеності ІС. Цей механізм заснований на підзвітності системи забезпечення безпеки, фіксує всі події, що стосуються безпеки, такі як:

- вхід і вихід суб'єктів доступу;
- запуск і завершення програм;
- видача друкованих документів;
- спроби доступу до ресурсів, що захищаються;
- зміна повноважень суб'єктів доступу;
- зміна статусу об'єктів доступу тощо.

Для систем, що сертифікуються з безпеки, інформаційних список контрольованих подій визначено галузевим документом «Положення про сертифікацію засобів і систем обчислювальної техніки і зв'язку за вимогами безпеки інформації».

Під протоколюванням розуміється збирання і накопичення інформації про події, що відбуваються в інформаційній системі. У кожного сервісу свій набір можливих подій, але в будь-якому випадку їх можна розділити на зовнішні (спричинені діями інших сервісів), внутрішні (викликані діями самого сервісу) і клієнтські (викликані діями користувачів і адміністраторів).

Ефективність системи безпеки принципово підвищується в разі доповнення механізму реєстрації механізмом аудиту. Це дозволяє оперативно виявляти порушення, визначати слабкі місця в системі захисту, аналізувати закономірності системи, оцінювати роботу користувачів тощо.

Аудит – це аналіз накопиченої інформації, що проводиться оперативно (в реальному часі) або періодично (наприклад, один раз

на день). Оперативний аудит з автоматичним реагуванням на виявлені нештатні ситуації називається активним.

Реалізація протоколювання і аудиту вирішує наступні завдання:

- забезпечення підзвітності користувачів і адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень інформаційної безпеки;
- надання інформації для виявлення і аналізу проблем.

Розглянуті вище механізми реєстрації та аудиту є потужним психологічним засобом, що нагадує потенційним порушникам про невідворотність покарання за несанкціоновані дії, а користувачам – за можливі критичні помилки.

Практичними засобами реєстрації та аудиту є:

- різні системні утиліти і прикладні програми;
- реєстраційний (системний або контрольний) журнал.

Перший засіб є зазвичай доповненням до моніторингу, що здійснюється адміністратором ІС. Комплексний підхід до протоколювання і аудиту забезпечується при використанні реєстраційного журналу.

Реєстраційний журнал – це хронологічно упорядкована сукупність записів результатів діяльності суб’єктів системи, що достатня для відновлення, перегляду та аналізу послідовності дій, які призводять до виконання операцій, процедур або подій при транзакції з метою контролю кінцевого результату.

Фрагмент журналу безпеки підсистеми реєстрації та аудиту операційної системи наведений на рис. 8.1.1.

Виявлення спроб порушень інформаційної безпеки входить у функції активного аудиту, завданнями якого є оперативне виявлення підозрілої активності та надання засобів для автоматичного реагування на неї.

Під підозрілою активністю розуміється поведінка користувача або компонента ІС, що є зловмисним (відповідно до заздалегідь визначеної політики безпеки) або нетиповим (згідно з прийнятими критеріями).

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	admin	GHJ

Рис. 8.1.1. Фрагмент журналу безпеки підсистеми реєстрації та аудиту ОС

Наприклад, підсистема аудиту, відстежуючи процедуру входу (реєстрації) користувача в систему підраховує кількість невдалих спроб входу. У разі перевищення встановленого порогу таких спроб підсистема аудиту формує сигнал про блокування облікового запису даного користувача.

Організація реєстрації подій, пов’язаних з безпекою інформаційної системи включає як мінімум три етапи:

1. Збирання і зберігання інформації про події.
2. Захист вмісту журналу реєстрації.
3. Аналіз вмісту журналу реєстрації.

На першому етапі визначаються дані, що підлягають збиранню та збереженню, період чистки і архівації журналу, ступінь централізації управління, місце і засоби зберігання журналу, можливість реєстрації шифрованої інформації та ін.

Реєстровані дані повинні бути захищені, в першу чергу, від несанкціонованої модифікації і, можливо, розкриття.

Найважливішим етапом є аналіз реєстраційної інформації. Відомі кілька методів аналізу інформації з метою виявлення несанкціонованих дій.

Статистичні методи засновані на накопиченні середньостатистичних параметрів функціонування підсистем і порівнянні поточних параметрів з ними. Наявність певних відхилень може сигналізувати про можливість появи деяких загроз.

Евристичні методи використовують моделі сценаріїв несанкціонованих дій, які описуються логічними правилами або

моделями дій, що за сукупністю призводять до несанкціонованих дій.

Протоколювання вимагає для своєї реалізації здорового глузду. Які події реєструвати? З яким ступенем деталізації? На подібні питання неможливо дати універсальні відповіді. Необхідно стежити за тим, щоб, з одного боку, досягалися перераховані вище цілі, а, з іншого, витрата ресурсів залишалася в межах допустимого. Занадто велике або докладне протоколювання не тільки знижує продуктивність сервісів (що негативно позначається на доступності), але і ускладнює аудит, тобто не збільшує, а зменшує інформаційну безпеку.

Розумний підхід до згаданих питань стосовно операційних систем пропонується в «Помаранчевій книзі», де виділені наступні події:

- вхід в систему (успішний чи ні);
- вихід з системи;
- звернення до віддаленої системи;
- операції з файлами (відкрити, закрити, перейменувати, видалення);
- зміна привілеїв чи інших атрибутів безпеки (режиму доступу, рівня благонадійності користувача і т.ін.).

При протоколюванні події рекомендується записувати наступну інформацію:

- дата і час події;
- унікальний ідентифікатор користувача – ініціатора дії;
- тип події;
- результат дії (успіх або невдача);
- джерело запиту (наприклад, ім’я терміналу);
- імена об’єктів (наприклад, що відкриваються або файлів, що видаляються);
- опис змін, внесених до баз даних захисту (наприклад, нова мітка безпеки об’єкта).

Ще одне важливе поняття, яке фігурує в «Помаранчевій книзі», – вибіркове протоколювання, як щодо користувачів (уважно стежити тільки за підозрілими), так і по відношенню до подій.

Характерна особливість протоколювання і аудиту – залежність від інших засобів безпеки. Ідентифікація та аутентифікація служать відправною точкою підзвітності користувачів, логічне керування доступом захищає конфіденційність і цілісність реєстраційної інформації. Можливо, для захисту залучаються і криптографічні методи.

Повертаючись до цілей протоколювання і аудиту, відзначимо, що забезпечення підзвітності важливе в першу чергу як стримуючий засіб. Якщо користувачі і адміністратори знають, що всі їхні дії фіксуються, вони, можливо, утримаються від незаконних операцій. Очевидно, якщо є підстави підозрювати будь-якого користувача в нечесності, можна реєструвати всі його дії, аж до кожного натискання клавіші. При цьому забезпечується не тільки можливість розслідування випадків порушення режиму безпеки, але і відкат некоректних змін (якщо в протоколі присутні дані до і після модифікації). Тим самим захищається цілісність інформації.

Реконструкція послідовності подій дозволяє виявити слабкі місця в захисті сервісів, дозволяє знайти винуватця вторгнення, оцінити масштаби завданих збитків та повернутися до нормальної роботи.

Виявлення спроб порушень інформаційної безпеки – функція активного аудиту. Звичайний аудит дозволяє виявити подібні спроби з запізненням, але і це виявляється корисним. Свого часу затримання німецьких хакерів, що діяли на замовлення КДБ, почалася з виявлення підозрілої розбіжності в кілька центів у щоденному звіті великого обчислювального центру.

Виявлення та аналіз проблем можуть допомогти поліпшити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переконфігурувати або переналаштувати систему, знову виміряти продуктивність тощо.

Непросто здійснити організацію узгодженого протоколювання і аудиту в розподіленій різнорідній системі. По-перше, деякі

компоненти, важливі для безпеки (наприклад, маршрутизатори), можуть не мати своїх ресурсів протоколювання. У такому випадку їх потрібно екранувати іншими сервісами, які візьмуть протоколювання на себе. По-друге, необхідно пов'язувати між собою події в різних сервісах.

8.1.1.1. Активний аудит

Під підозрілою активністю розуміється поведінка користувача або компонента інформаційної системи, що є зловмисним (відповідно до заздалегідь визначеної політики безпеки) або нетиповим (згідно з прийнятими критеріями).

Завдання активного аудиту – оперативно виявляти підозрілу активність і надавати засоби для автоматичного реагування на неї.

Активність, яка не відповідає політиці безпеки, доцільно розділити на атаки, спрямовані на незаконне отримання повноважень, і на дії, що виконуються в межах наявних повноважень, але порушують політику безпеки.

Атаки порушують будь-яку осмислену політику безпеки. Іншими словами, активність атакуючого є руйнівною незалежно від політики. Отже, для опису і виявлення атак можна застосовувати універсальні методи, інваріантні щодо політики безпеки, такі як сигнатури і їх виявлення у вхідному потоці подій за допомогою апарату експертних систем.

Сигнатура атаки – це сукупність умов, при виконанні яких вважається, що має місце атака, що викликає заздалегідь визначену реакцію. Найпростіший приклад сигнатури – «зафіксовані три послідовні невдалі спроби входу в систему з одного терміналу» є прикладом асоційованої реакції – блокування терміналу до прояснення ситуації.

Дії, що виконуються в межах наявних повноважень, але порушують політику безпеки, ми будемо називати зловживанням повноваженнями. Зловживання повноваженнями можливі через неадекватність засобів розмежування доступу обраної політики

безпеки. Найпростішим прикладом зловживань є неетична поведінка суперкористувача, що переглядає особисті файли інших користувачів. Аналізуючи реєстраційну інформацію, можна виявити подібні події і повідомити про них адміністратору безпеки, хоча для цього необхідні відповідні засоби вираження політики безпеки.

Виділення зловживань повноваженнями в окрему групу неправомірних дій, що виявляються засобами активного аудиту, не є загальноприйнятим, однак, на наш погляд, подібний підхід має право на існування і ми будемо його дотримуватися, хоча найбільш радикальним рішенням був би розвиток засобів розмежування доступу.

Нетипова поведінка виявляється статистичними методами. У найпростішому випадку застосовують систему порогів, перевищення яких є підозрілим, хоча «пороговий» метод можна трактувати і як вироджений випадок сигнатури атаки, і як тривіальний спосіб вираження політики безпеки. У більш розвинених системах здійснюється зіставлення довготривалих характеристик роботи (довгострокових профілів) з короткостроковими профілями. У цьому випадку можна провести аналогію біометричної аутентифікації за поведінковими характеристиками.

Стосовно до засобів активного аудиту розрізняють помилки першого і другого роду: пропуск атак і помилкові тривоги, відповідно. Небажаність помилок першого роду очевидна; помилки другого роду не менше неприємні, оскільки відволікають адміністратора безпеки від дійсно важливих справ, побічно сприяючи пропуску атак.

Переваги сигнатурного методу – висока продуктивність, мале число помилок другого роду, обґрунтованість рішень. Основний недолік – невміння виявляти невідомі атаки і варіації відомих атак.

Основні переваги статистичного підходу – універсальність і обґрунтованість рішень, потенційна здатність виявляти невідомі атаки, тобто мінімізація числа помилок першого роду. Мінуси полягають у відносно високій частці помилок другого роду, погану

роботу в разі, коли неправомірна поведінка є типовою, коли типова поведінка плавно змінюється від легальної до неправомірної, а також у випадках, коли типової поведінки немає (як показує статистика, таких користувачів приблизно 5-10%).

Засоби активного аудиту можуть розташовуватися на всіх лініях оборони інформаційної системи. На межі контрольованої зони вони можуть виявляти підозрілу активність у точках підключення до зовнішніх мереж (не тільки спроби нелегального проникнення, але і дії по «промацуванню» сервісів безпеки). У корпоративній мережі, в межах інформаційних сервісів і сервісів безпеки, активний аудит у змозі виявити і припинити підозрілу активність зовнішніх і внутрішніх користувачів, виявити проблеми в роботі сервісів, які викликані як порушеннями безпеки, так і апаратно-програмними помилками. Важливо відзначити, що активний аудит, в принципі, здатний забезпечити захист від атак на доступність.

На жаль, формулювання «в принципі, здатний забезпечити захист» виник не випадково. Активний аудит розвивається десятки років, і перші результати здавалися досить багатообіцяючими. Досить швидко вдалося реалізувати розпізнавання простих типових атак, проте потім було виявлено безліч проблем, пов’язаних з виявленням заздалегідь невідомих, розподілених, розтягнутих у часі і інших атак. Було б наївно очікувати повного вирішення подібних проблем найближчим часом (оперативне поповнення бази сигнатур атак, звичайно, не є таким рішенням). Проте, і на нинішній стадії розвитку, активний аудит корисний як один з рубежів (вірніше, як набір прошарків) ешелонованої оборони.

8.1.1.2. Функціональні компоненти і архітектура

У складі засобів активного аудиту можна виділити наступні функціональні компоненти:

• компоненти генерації реєстраційної інформації. Вони знаходяться на рубежі між засобами активного аудиту та контрольованими об’єктами;

• компоненти зберігання згенерованої реєстраційної інформації;

• компоненти вилучення реєстраційної інформації (сенсори). Зазвичай розрізняють мережеві і хостові сенсори, маючи на увазі під першими виділені комп’ютери, мережеві карти яких встановлені в режим прослуховування, а під другими – програми, які читають реєстраційні журнали операційної системи. На наш погляд, з розвитком комутаційних технологій ця різниця поступово стирається, так як мережеві сенсори доводиться встановлювати в активному мережному обладнанні і, по суті, вони стають частиною мережевої ОС;

• компоненти перегляду реєстраційної інформації. Можуть допомогти при прийнятті рішення про реагування на підозрілу активність;

• компоненти аналізу інформації, що надійшла від сенсорів. Відповідно до цього визначення засобів активного аудиту, виділяють пороговий аналізатор, аналізатор порушень політики безпеки, експертну систему, що виявляє сигнатури атак, а також статистичний аналізатор, який виявляє нетипову поведінку;

• компоненти зберігання інформації, яка бере участь в аналізі. Таке зберігання необхідно, наприклад, для виявлення атак, розтягнених у часі;

• компоненти прийняття рішень і реагування («вирішувачі»). «Вирішувач» може отримувати інформацію не тільки від локальних, а й від зовнішніх аналізаторів, проводячи так званий кореляційний аналіз розподілених подій;

• компоненти зберігання інформації про контрольовані об’єкти. Тут можуть зберігатися як пасивні дані, так і методи, необхідні, наприклад, для вилучення з об’єкта реєстраційної інформації для реагування;

• компоненти, які відіграють роль організуючої оболонки для менеджерів активного аудиту, називаються моніторами і

об’єднують аналізатори, «вирішувачі», сховище описів об’єктів і інтерфейсні компоненти. У число останніх входять компоненти інтерфейсу з іншими моніторами, як рівноправними, так і тими, що входять в ієрархію. Такі інтерфейси необхідні, наприклад, для виявлення розподілених, широкомасштабних атак;

- компоненти інтерфейсу з адміністратором безпеки.

Засоби активного аудиту будуються в архітектурі менеджер/агент. Основними агентськими компонентами є сенсори. Аналіз, прийняття рішень – функції менеджерів. Очевидно, між менеджерами та агентами повинні бути сформовані довірені канали.

Підкреслимо важливість інтерфейсних компонентів. Вони корисні як з внутрішньої для засобів активного аудиту точки зору (забезпечують розширюваність, підключення компонентів різних виробників), так і з зовнішньої точки зору. Між менеджерами (між компонентами аналізу і «вирішувачем») можуть існувати горизонтальні зв’язки, необхідні для аналізу розподіленої активності. Можливо також формування ієрархій засобів активного аудиту з винесенням на верхні рівні інформації про найбільш масштабну та небезпечну активність.

Звернемо також увагу на архітектурну спільність засобів активного аудиту та управління, що є наслідком спільності виконуваних функцій. Продумані інтерфейсні компоненти можуть істотно полегшити спільну роботу цих засобів.

8.1.2. Шифрування

Криптографія – це наука про забезпечення безпеки даних, що забезпечує рішення чотирьох важливих проблем безпеки: конфіденційності, аутентифікації, цілісності і контролю учасників взаємодії.

Криптографія необхідна для реалізації сервісів безпеки: шифрування; контроль цілісності; аутентифікація (цей сервіс був розглянутий нами раніше).

Найнадійніший технічний метод інформаційної безпеки заснований на використанні криптосистем. Криптосистема включає:

- алгоритм шифрування;
- набір ключів (послідовність двійкових чисел), які використовуються для шифрування;
- систему управління ключами.

Загальна схема роботи криптосистеми показана рис. 8.1.2.

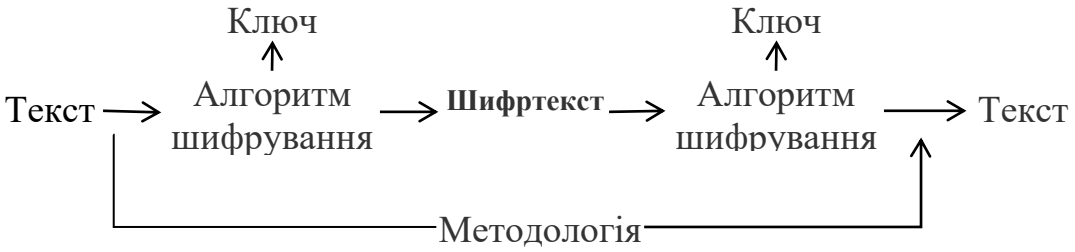


Рис. 8.1.2. Схема роботи криптосистеми

Криптосистеми вирішують такі проблеми ІБ як забезпечення конфіденційності, цілісності даних, аутентифікацію даних і їх джерел.

Криптографічні методи захисту є обов'язковим елементом безпечних інформаційних систем. Особливе значення криптографічні методи отримали з розвитком розподілених відкритих мереж, в яких немає можливості забезпечити фізичний захист каналів зв'язку.

Шифрування – це перетворення даних у форму, яку неможливо прочитати без використання ключів шифрування-розшифровки. Шифрування дозволяє забезпечити конфіденційність, зберігаючи інформацію в таємниці від того, кому вона не призначена.

Шифрування є найбільш потужним засобом забезпечення конфіденційності. Багато в чому воно займає центральне місце серед програмно-технічних регуляторів безпеки, основою реалізації багатьох з них, і в той же час останнім (а часом і єдиним) захисним

кордоном. Наприклад, для портативних комп'ютерів тільки шифрування дозволяє забезпечити конфіденційність даних навіть у разі крадіжки.

У більшості випадків і шифрування, і контроль цілісності відіграють глибоко інфраструктурну роль, залишаючись прозорими і для додатків, і для користувачів. Типове місце цих сервісів безпеки – на мережевому і транспортному рівнях реалізації стека мережевих протоколів.

Основною класифікаційною ознакою систем шифрування даних є спосіб їх функціонування. За способом функціонування системи шифрування даних поділяють на два класи:

- системи «прозорого» шифрування;
- системи, спеціально викликані для здійснення шифрування.

В системах «прозорого» шифрування (шифрування «з льоту») криптографічні перетворення здійснюються в режимі реального часу, непомітно для користувача. Наприклад, користувач записує підготовлений у текстовому редакторі документ на об'єкт, що захищається, а система захисту в процесі запису виконує його шифрування. Системи другого класу зазвичай являють собою утиліти (програми), які необхідно спеціально викликати для виконання шифрування.

Як уже зазначалося, особливе значення криптографічні перетворення мають місце при передаванні даних по розподілених обчислювальних мережах. Для захисту даних у розподілених мережах використовуються два підходи: канальне шифрування і кінцеве (абонентське) шифрування.

У разі канального шифрування захищається вся інформація, що передається по каналу зв'язку, включаючи службову. Цей спосіб шифрування має наступну перевагу – вбудовування процедур шифрування на канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи.

Кінцеве (абонентське) шифрування дозволяє забезпечити конфіденційність даних, що передаються між двома абонентами. У

цьому випадку захищається тільки зміст повідомлень, а вся службова інформація залишається відкритою.

Розрізняють два основні методи шифрування: симетричний (шифрування секретним ключем) і асиметричний (шифрування відкритим ключем). У першому з них один і той же ключ (що зберігається в секреті) використовується і для шифрування, і для розшифрування даних.

Розроблено достатньо ефективні (швидкі і надійні) методи симетричного шифрування. Загальна технологія використання симетричного методу шифрування представлена на рис. 8.1.3.

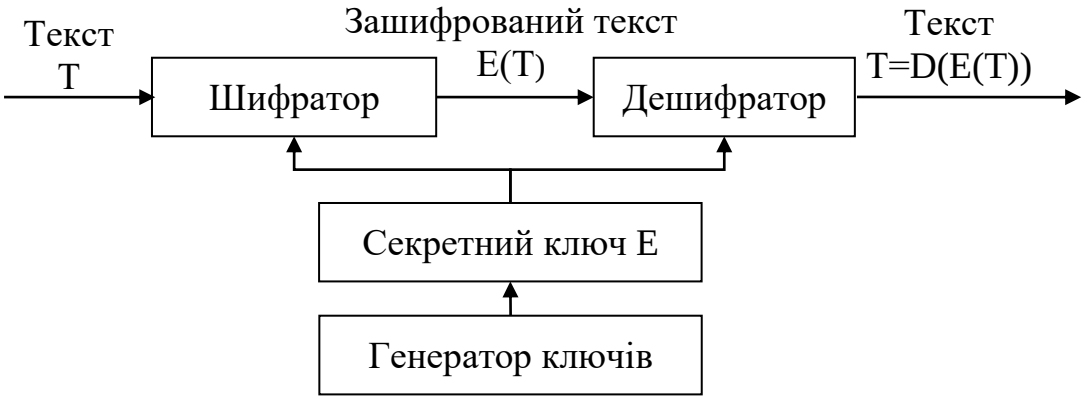


Рис. 8.1.3. Використання симетричного методу шифрування

Найбільш відомим стандартом на симетричне шифрування із закритим ключем є стандарт для оброблення інформації в державних установах США DES (Data Encryption Standard). Існують і інші стандарти на подібні методи (наприклад, ГОСТ 28147-89 «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення»).

Для більшої визначеності ми будемо вести мову про захист повідомлень, хоча події можуть розвиватися не тільки в просторі, але і в часі, коли зашифровуються і розшифровуються файли, що нікуди не переміщаються.

Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий і відправнику, і одержувачу. З одного боку, це створює нову проблему поширення ключів. З

іншого боку, одержувач на підставі наявності зашифрованого і розшифрованого повідомлення не може довести, що він отримав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати самостійно.

Це істотно ускладнює процедуру призначення і розподілу ключів між користувачами. Зазначений недолік послужив причиною розробки методів шифрування з відкритим ключем – асиметричних методів (рис. 8.1.4).

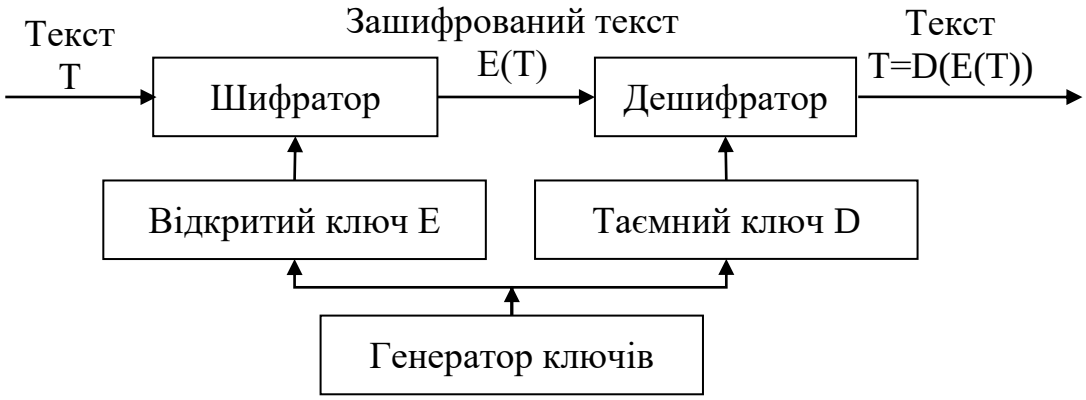


Рис. 8.1.4. Використання асиметричного методу шифрування

В асиметричних методах використовуються два ключа. Один з них, несекретний (він може публікуватися разом з іншими відкритими відомостями про користувача), що застосовується для шифрування, інший (секретний, відомий тільки одержувачу) – для розшифрування. В наш час найбільш відомим і надійним є асиметричний алгоритм RSA (Райвест (Rivest), Шамір (Shamir), Адлеман (Adleman)), заснований на операціях з великими (наприклад, 100-значними) простими числами і їх добутками.

Істотним недоліком асиметричних методів шифрування є їхня низька швидкодія, тому дані методи доводиться поєднувати з симетричними (асиметричні методи на 3-4 порядки повільніше). Рис. 8.1.5 ілюструє шифрування, реалізоване шляхом поєднання симетричного і асиметричного методів.

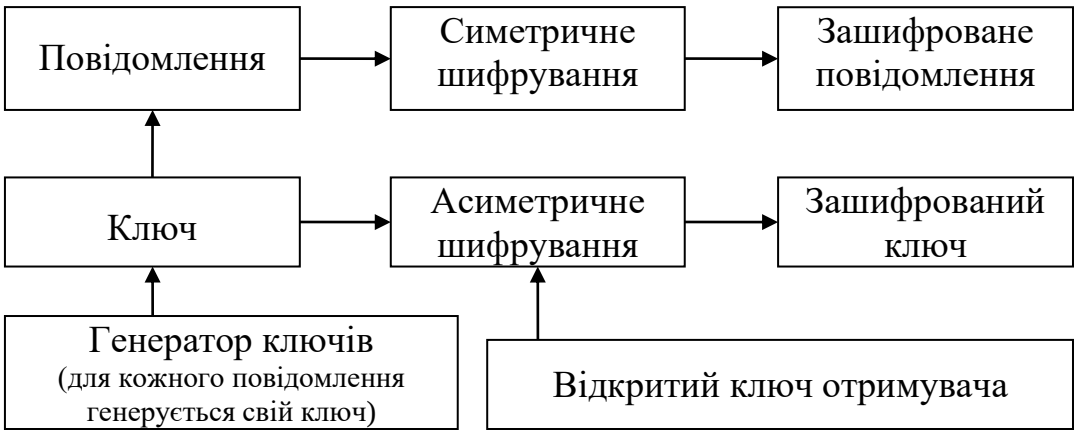


Рис. 8.1.5. Шифрування повідомлення шляхом поєднання симетричного і асиметричного методів

У цьому випадку, для вирішення завдання ефективного шифрування з передачею секретного ключа, що використовується відправником, повідомлення спочатку симетрично зашифровують випадковим ключем, потім цей ключ зашифровують відкритим асиметричним ключем одержувача, після чого повідомлення і ключ відправляються по мережі. На рис. 8.1.6 показано розшифрування зашифрованого повідомлення.

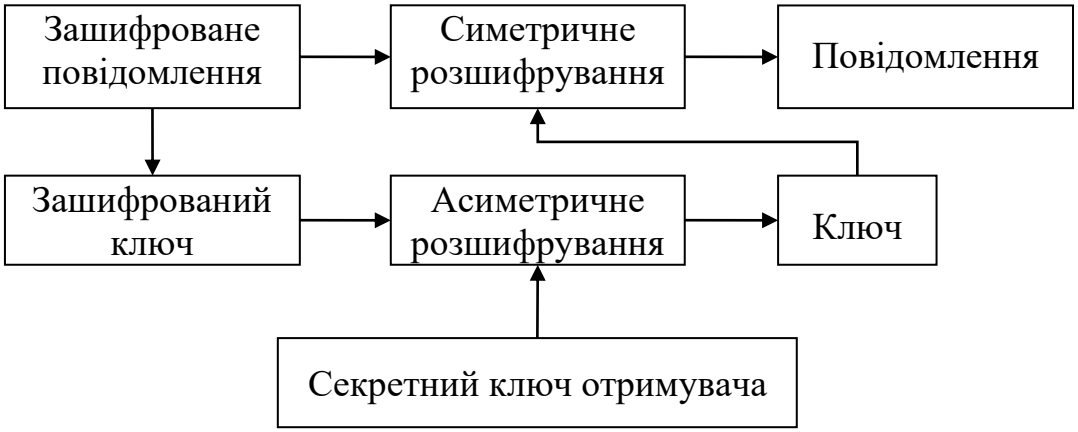


Рис. 8.1.6. Розшифрування ефективно зашифрованого повідомлення

Відзначимо, що асиметричні методи дозволили вирішити важливе завдання спільного формування секретних ключів (це істотно, якщо сторони не довіряють одна одній), які обслуговують

сеанс взаємодії, при первісній відсутності загальних секретів. Для цього використовується алгоритм Діффі-Хелмана.

Певного поширення набув різновид симетричного шифрування, заснований на використанні складених ключів. Ідея полягає в тому, що секретний ключ ділиться на дві частини, що зберігаються окремо. Кожна частина сама по собі не дозволяє виконати розшифрування. Якщо у правоохоронних органів з'являються підозри щодо особи, яка використовує деякий ключ, вони можуть в установленому порядку отримати половинки ключа і далі діяти звичайним для симетричного розшифрування чином.

Порядок роботи зі складеними ключами – хороший приклад реалізації принципу розподілу обов'язків. Він дозволяє поєднувати права на різного роду таємниці (персональну, комерційну) з можливістю ефективно стежити за порушниками закону, хоча, звичайно, тут дуже багато тонкощів і технічного, і юридичного плану.

Багато криптографічних алгоритмів у якості одного з параметрів вимагають псевдовипадкове значення, в разі передбачуваності якого в алгоритмі з'являється уразливість (подібне вразливе місце було виявлено в деяких варіантах Web-навігаторів). Генерація псевдовипадкових послідовностей є важливим аспектом криптографії.

8.1.3. Контроль цілісності

Криптографічні методи дозволяють надійно контролювати цілісність як окремих порцій даних, так і їх наборів (таких як потік повідомлень); визначати справжність джерела даних; гарантувати неможливість відмовитися від виконаних дій («безвідмовності»).

В основі криптографічного контролю цілісності лежать два поняття:

- хеш-функція;
- електронний цифровий підпис (ЕЦП).

Хеш-функція – це перетворення даних (одностороння функція), що реалізовується, як правило, засобами симетричного шифрування зі зв'язуванням блоків. Результат шифрування

останнього блоку (залежить від всіх попередніх) і служить результатом хеш-функції.

Нехай є дані, цілісність яких потрібно перевірити, хеш-функція і раніше обчислений результат її застосування до вихідних даних (так званий дайджест). Позначимо хеш-функцію через h, вихідні дані – через T, перевіряються дані – через T'. Контроль цілісності даних зводиться до перевірки рівняння h(T') = h(T). Якщо воно виконано, вважається, що T'= T. Збіг дайджестів для різних даних називається колізією. В принципі, колізії, звичайно, можливі, оскільки потужність множини дайджестів менше, ніж потужність множини даних, що хешуються, однак те, що h є односторонньою функцією, означає, що за прийнятний час спеціально організувати колізію неможливо.

Електронний цифровий підпис є відносно невеликою кількістю додаткової аутентифікуючої інформації, що передається разом з підписаним текстом. Відправник формує цифровий підпис, використовуючи секретний ключ відправника. Одержувач перевіряє підпис, використовуючи відкритий ключ відправника.

Ідея технології електронного підпису полягає в наступному. Відправник передає два примірники одного повідомлення: відкрите і розшифроване його закритим ключем (тобто зворотно шифроване). Одержувач шифрує за допомогою відкритого ключа відправника розшифрований екземпляр. Якщо він співпаде з відкритим варіантом, то особистість і підпис відправника вважається встановленою.

При практичній реалізації електронного підпису також шифрується не всі повідомлення, а лише спеціальна контрольна сума – хеш, що захищає послання від нелегальної зміни. Електронний підпис тут гарантує як цілісність повідомлення, так і засвідчує особу відправника.

Розглянемо більш докладно застосування асиметричного шифрування для формування і перевірки електронного цифрового підпису.

Нехай E(T) позначає результат шифрування тексту T за допомогою відкритого ключа, а D(T) – результат розшифрування тексту T (як правило, зашифрованого) за допомогою секретного

ключа. Щоб асиметричний метод міг застосовуватися для реалізації ЕЦП, необхідно виконання тотожності

E(D(T)) = D(E(T)) = T.

З рівняння E(S') = h(T') випливає, що S' = D(h(T') (для доказу досить застосувати до обох частин перетворення D і викреслити в лівій частині тотожне перетворення D(E())). Таким чином, електронний цифровий підпис захищає цілісність повідомлення та засвідчує особу відправника.

Процедура формування електронного цифрового підпису, що складається в шифруванні перетворенням D дайджесту h(T) показана на рис. 8.1.7.

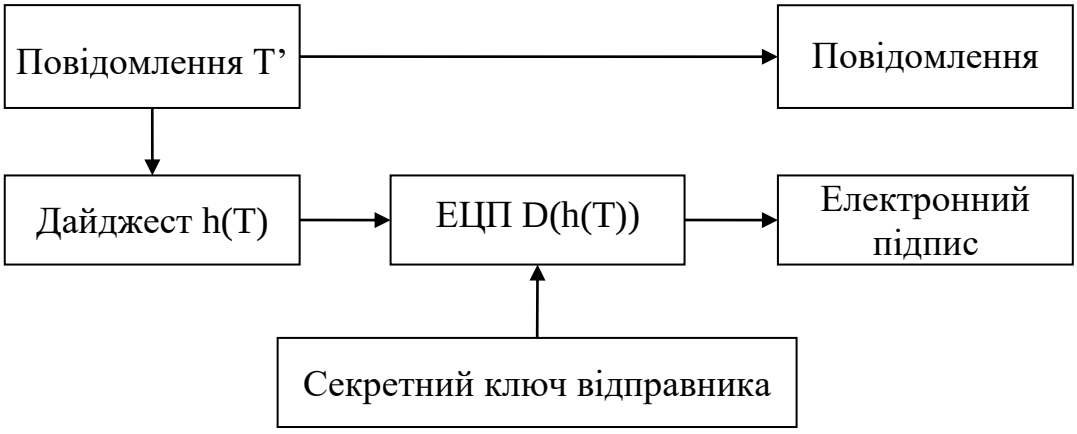


Рис. 8.1.7. Формування електронного цифрового підпису

Перевірка ЕЦП може бути реалізована так, як показано на рис. 8.1.8.

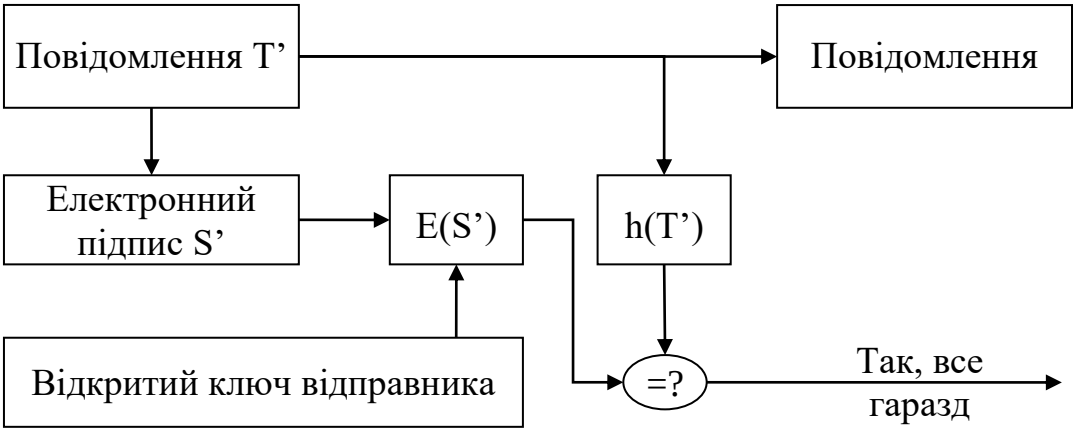


Рис. 8.1.8. Перевірка електронного цифрового підпису

Два стандарти, ГОСТ Р 34.10-94 «Процедури формування і перевірки електронного цифрового підпису на базі асиметричного криптографічного алгоритму» і ГОСТ Р 34.11-94 «Функція хешування», об'єднані загальним заголовком «Інформаційна технологія. Криптографічний захист інформації», регламентують обчислення дайджесту і реалізацію ЕЦП.

Для контролю цілісності послідовності повідомлень (тобто для захисту від крадіжки, дублювання і переупорядковування повідомлень) застосовують часові штампи і нумерацію елементів послідовності, при цьому штампи і номера включають в текст, що підписується.

8.1.3.1. Цифрові сертифікати

При використанні асиметричних методів шифрування (і, зокрема, електронного цифрового підпису) необхідно мати гарантію автентичності пари (ім'я користувача, відкритий ключ користувача), так як безпека будь-якої криптосистеми визначається криптографічними ключами, що використовуються. У разі ненадійного управління ключами зловмисник може заволодіти ключовою інформацією і отримати повний доступ до всієї інформації в системі або мережі.

Розрізняють такі види функцій управління ключами: генерація, зберігання і розподіл ключів.

Способи генерації ключів для симетричних і асиметричних криптосистем різні. Для генерації ключів симетричних криптосистем використовуються апаратні і програмні засоби генерації випадкових чисел. Генерація ключів для асиметричних криптосистем складніша, тому, що ключі повинні володіти певними математичними властивостями.

Функція зберігання передбачає організацію безпечного зберігання, обліку та видалення ключової інформації. Для забезпечення безпечного зберігання ключів застосовують їх шифрування за допомогою альтернативних джерел. Такий підхід

призводить до концепції ієрархії ключів. У ієрархію ключів зазвичай входить головний ключ (тобто майстер-ключ), ключ шифрування ключів і ключ шифрування даних. Слід зазначити, що генерація і зберігання майстер-ключа є найбільш критичним питанням криптозахисту.

Розподіл – найвідповідальніший процес в управлінні ключами. Цей процес повинен гарантувати таємність ключів, що розподіляються, а також бути оперативним і точним. Між користувачами мережі ключі розподіляють за допомогою прямого обміну сеансовими ключами або використовуючи один або кілька центрів розподілу ключів.

Для вирішення цього завдання в специфікаціях X.509 вводяться поняття цифрового сертифікату та центру сертифікації (засвідчення справжності).

• Центр сертифікації – це компонент глобальної служби каталогів, що відповідає за управління криптографічними ключами користувачів. Відкриті ключі та інша інформація про користувачів зберігається засвідчують центрами у вигляді цифрових сертифікатів, що мають наступну структуру:

• порядковий номер сертифіката;

• ідентифікатор алгоритму електронного підпису;

• ім’я центру посвідчення;

• термін придатності;

• ім’я власника сертифіката (ім’я користувача, якому належить сертифікат);

• відкриті ключі власника сертифіката (ключів може бути кілька);

• ідентифікатори алгоритмів, асоційованих з відкритими ключами власника сертифіката;

• електронний підпис, що згенерований з використанням секретного ключа центру сертифікації (підписується результат хешування всієї інформації, що зберігається в сертифікаті).

Цифрові сертифікати мають такі властивості:

• будь-який користувач, що знає відкритий ключ центру сертифікації, може дізнатися відкриті ключі інших клієнтів центру і перевірити цілісність сертифіката;

• ніхто, крім центру сертифікації не може модифікувати інформацію про користувача без порушення цілісності сертифікату.

У специфікаціях X.509 не описується конкретна процедура генерації криптографічних ключів та управління ними, однак даються деякі загальні рекомендації. Зокрема, зазначається, що пари ключів можуть здійснюватися будь-яким з наступних способів.

• ключі може генерувати сам користувач. У такому випадку секретний ключ не потрапляє в руки третіх осіб, проте потрібно вирішувати задачу безпечного зв'язку з центром сертифікації;

• ключі генерує довірена особа. У такому випадку доводиться вирішувати завдання безпечної доставки секретного ключа власнику і надання довірених даних для створення сертифіката;

• ключі генеруються центром сертифікації. В такому випадку залишається тільки завдання безпечної передачі ключів власнику.

Цифрові сертифікати у форматі X.509 стали не тільки формальним, але і фактичним стандартом, що підтримується численними центрами сертифікації.

Тема 8.2. Екранування і тунелювання

8.2.1. Екранування

Одним з ефективних механізмом забезпечення інформаційної безпеки розподілених обчислювальних мереж є екранування, яке виконує функції розмежування інформаційних потоків на межі мережі, що захищається.

Міжмережеве екранування підвищує безпеку об'єктів внутрішньої мережі за рахунок ігнорування неавторизованих запитів із зовнішнього середовища, тим самим, забезпечуючи всі складові інформаційної безпеки. Крім функцій розмежування доступу, екранування забезпечує реєстрацію інформаційних обмінів.

Функції екранування виконує міжмережевий екран (МЕ) або брандмауер (firewall), під яким розуміють програмну або програмно-апаратну систему, яка виконує контроль інформаційних потоків, що надходять в інформаційну систему і/або виходять з неї, і забезпечує захист інформаційної системи за допомогою фільтрації інформації. Фільтрація інформації полягає в аналізі інформації за сукупністю критеріїв та прийнятті рішення про її прийняття і/або передачу.

Формальна постановка задачі екранування полягає в наступному. Нехай є дві множини інформаційних систем.

Екран – це засіб розмежування доступу клієнтів з однієї множини до серверів з іншої множини. Екран здійснює свої функції, контролюючи усі інформаційні потоки між двома множинами систем (рис. 8.2.1).

Контроль потоків полягає в їх фільтрації, можливо, з виконанням деяких перетворень.

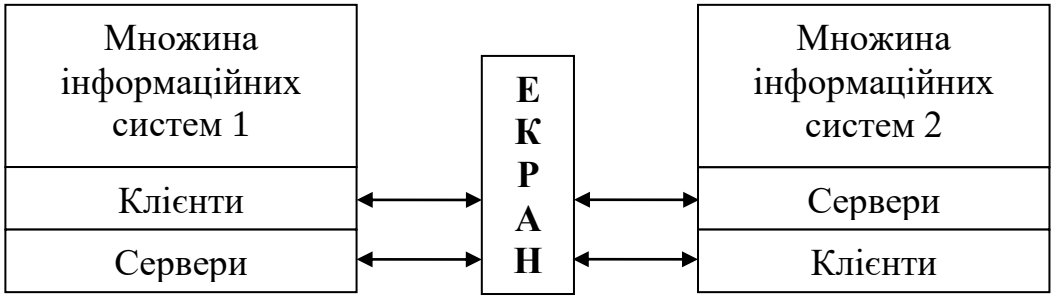


Рис. 8.2.1. Екран як засіб розмежування доступу

На наступному рівні деталізації екран (напівпроникну мембрану) зручно представляти як послідовність фільтрів. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу «перекинути» за екран. Крім того, допускається перетворення даних, передавання порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата і повернення результату відправнику (рис. 8.2.2).

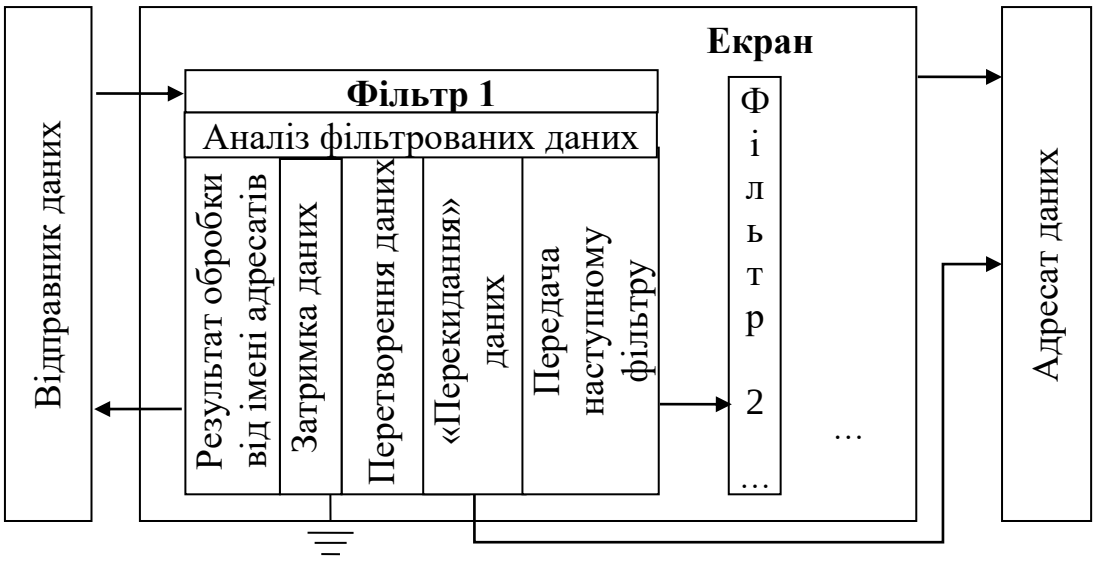


Рис. 8.2.2. Екран як послідовність фільтрів

Крім функцій розмежування доступу, екрани здійснюють протоколювання обміну інформацією.

Зазвичай екран не є симетричним, для нього визначені поняття «всередині» і «зовні». При цьому завдання екранування формулюється як захист внутрішньої області від потенційно ворожої зовнішньої. Так, міжмережеві екрани найчастіше встановлюють для захисту корпоративної мережі організації, що має вихід в Internet.

Екранування допомагає підтримувати доступність сервісів внутрішньої області, зменшуючи або взагалі ліквідовуючи навантаження, що викликається зовнішньою активністю. Зменшується вразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен подолати екран, де захисні механізми сконфігуровані особливо ретельно. Крім того, екрануюча система, на відміну від універсальної, може бути влаштована більш простим і, отже, більш безпечним чином.

Екранування дає можливість контролювати також інформаційні потоки, спрямовані в зовнішню область, що сприяє підтримці режиму конфіденційності в ІС організації.

Підкреслимо, що екранування може використовуватися як сервіс безпеки не тільки в мережевому, а й в будь-якому іншому середовищі, де відбувається обмін повідомленнями. Найважливіший приклад подібного середовища – об’єктно-орієнтовані програмні системи, коли для активізації методів об’єктів виконується (в концептуальному плані) передача повідомлень. Досить імовірно, що в майбутніх об’єктно-орієнтованих середовищах екранування стане одним з найважливіших інструментів розмежування доступу до об’єктів.

Екранування може бути частковим, тобто таким, що захищає певні інформаційні сервіси.

Обмежуючий інтерфейс також можна розглядати як різновид екранування. На невидимий об’єкт важко нападати, особливо за допомогою фіксованого набору засобів. У цьому сенсі Web-інтерфейс має природний захист, особливо у тому випадку, коли гіпертекстові документи формуються динамічно. Кожен користувач бачить лише те, що йому належить бачити. Можна провести аналогію між гіпертекстовими документами, що динамічно

формуються і представленнями в реляційних базах даних, з тією ж суттєвою різницею, що у випадку з Web можливості істотно ширше.

Екрануюча роль Web-сервісу наочно проявляється і тоді, коли цей сервіс здійснює посередницькі (точніше, інтегруючі) функції при доступі до інших ресурсів, наприклад таблиць бази даних. У цьому випадку не тільки контролюються потоки запитів, а й приховується реальна організація даних.

8.2.1.1. Архітектурні аспекти міжмережевих екранів

Боротися з загрозами, властивими мережному середовищу, засобами універсальних операційних систем не представляється можливим. Універсальна ОС – це величезна програма, що напевно містить, крім явних помилок, деякі особливості, які можуть бути використані для нелегального отримання привілеїв. Сучасна технологія програмування не дозволяє зробити настільки великі програми безпечними. Крім того, адміністратор, який має справу зі складною системою, далеко не завжди у змозі врахувати всі наслідки проведених змін. Нарешті, в універсальній системі проломи в безпеці постійно створюються самими користувачами (слабкі і/або рідко змінювані паролі, невдало встановлені права доступу, залишений без догляду термінал тощо). Єдиний перспективний шлях пов’язаний з розробкою спеціалізованих сервісів безпеки, які в силу своєї простоти допускають формальну чи неформальну верифікацію. Брандмауер якраз і є таким засобом, що допускає подальшу декомпозицію, пов’язану з обслуговуванням різних мережевих протоколів.

Міжмережевий екран розташовується між мережею, що захищається (внутрішньою мережею) і зовнішнім середовищем (зовнішніми мережами іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, у другому – про внутрішній. Залежно від точки зору, зовнішній МЕ можна вважати першою або останньою (але ніяк не єдиною) лінією оборони.

Першою – якщо дивитися на світ очима зовнішнього зловмисника. Останньою – якщо прагнути до захищеності всіх компонентів корпоративної мережі та припинення неправомірних дій внутрішніх користувачів.

Брандмауер – ідеальне місце для вбудовування засобів активного аудиту. З одного боку, і на першому, і на останньому захисному рубежі виявлення підозрілої активності по-своєму важливо. З іншого боку, МЕ здатний реалізувати як завгодно потужну реакцію на підозрілу активність, аж до розриву зв'язку із зовнішнім середовищем. Правда, потрібно мати на увазі, що з'єднання двох сервісів безпеки в принципі може створити пролом, який сприяє атакам на доступність.

На міжмережевий екран доцільно покласти ідентифікацію/аутентифікацію зовнішніх користувачів, які потребують доступу до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

В силу принципів ешелонування оборони для захисту зовнішніх підключень зазвичай використовується двокомпонентне екранування (рис. 8.2.3). Первинна фільтрація (наприклад, блокування пакетів управляючого протоколу SNMP, небезпечного атаками на доступність, або пакетів з певними IP-адресами, включеними в «чорний список») здійснюється граничним маршрутизатором, за яким розташовується так звана демілітаризована зона (мережа з помірним рівнем безпеки, куди виносяться зовнішні інформаційні сервіси організації – Web, електронна пошта тощо) і основний МЕ, що захищає внутрішню частину корпоративної мережі.

Теоретично міжмережевий екран (особливо внутрішній) повинен бути багатопротокольним, однак на практиці домінування сімейства протоколів TCP/IP настільки велике, що підтримка інших протоколів представляється надмірністю, шкідливою для безпеки (складніший сервіс більш вразливий).

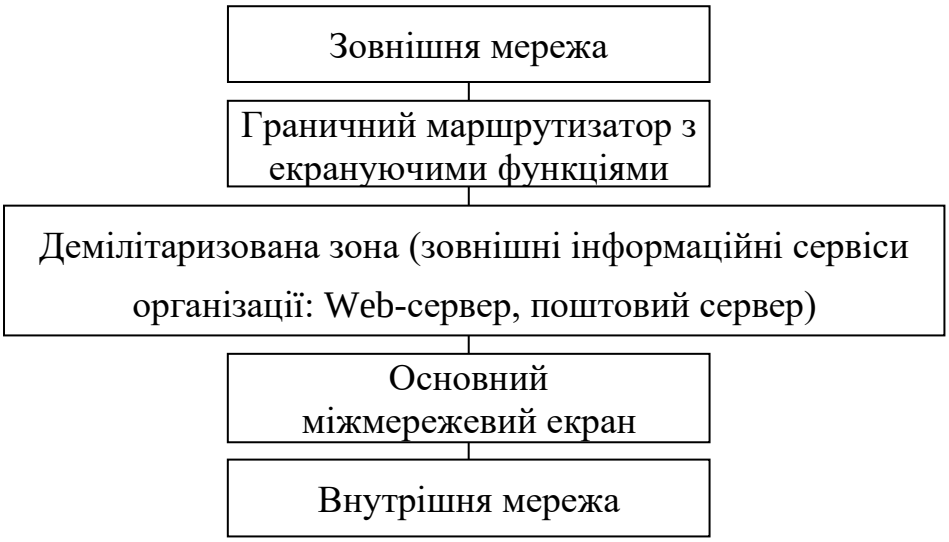


Рис. 8.2.3. Двокомпонентне екранування з демілітаризованою зоною

Взагалі кажучи, і зовнішній, і внутрішній міжмережевий екран може стати вузьким місцем, оскільки обсяг мережевого трафіку має тенденцію швидкого зростання. Один з підходів до вирішення цієї проблеми передбачає розбиття МЕ на кілька апаратних частин і організацію спеціалізованих серверів-посередників. Основний міжмережевий екран може проводити грубу класифікацію вхідного трафіку за видами і передоручати фільтрацію відповідним посередникам (наприклад, посереднику, що аналізує HTTP-трафік). Вихідний трафік спочатку обробляється сервером-посередником, який може виконувати і функціонально корисні дії, такі як кешування сторінок зовнішніх Web-серверів, що знижує навантаження на мережу взагалі і основний МЕ зокрема.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є скоріше винятком, ніж правилом. Навпаки, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожен з яких підключений до Internet. У цьому випадку кожне підключення має захищатися своїм екраном. Точніше кажучи, можна вважати, що корпоративний зовнішній міжмережевий екран є складеним, і

потрібно вирішувати задачу погодженого адміністрування (управління та аудиту) всіх компонентів.

Протилежністю складеним корпоративним МЕ (або їх компонентами) є персональні міжмережеві екрани і персональні екрануючі пристрої. Перші є програмними продуктами, які встановлюються на персональні комп'ютери і захищають тільки їх. Другі реалізуються на окремих пристроях і захищають невелику локальну мережу, таку як мережа домашнього офісу.

При розгортанні міжмережевих екранів слід дотримуватися розглянутих нами раніше принципи архітектурної безпеки, в першу чергу подбавши про простоту і керованість, про ешелонування оборони, а також про неможливість переходу в небезпечний стан. Окрім того, слід брати до уваги не тільки зовнішні, але і внутрішні загрози.

8.2.1.2. Класифікація міжмережевих екранів

Міжмережеві екрани класифікуються за такими ознаками:

- за місцем розташування в мережі – на зовнішні і внутрішні, що забезпечують захист відповідно від зовнішньої мережі або захист між сегментами мережі;
- за рівнем фільтрації, що відповідає рівню еталонної моделі OSI/ISO.

Зовнішні міжмережеві екрани зазвичай працюють тільки з протоколом TCP/IP глобальної мережі Інтернет. Внутрішні мережеві екрани можуть підтримувати декілька протоколів, наприклад, при використанні мережевої операційної системи Novell Netware, слід брати до уваги протокол SPX/IPX.

При розгляді будь-якого питання, що стосується мережевих технологій, основою служить еталонна модель ISO/OSI. Міжмережеві екрани також доцільно класифікувати за рівнем фільтрації – канальним, мережним, транспортним чи прикладним (табл. 8.1).

Таблиця 8.1

Типи міжмережевих екранів і рівні моделі ISO OSI

	Рівень моделі OSI	Протокол	Тип брандмауера
1	Прикладний	Telnet, FTP, DNS, NFS, SMTP, HTTP	шлюз прикладного рівня; міжмережевий екран експертного рівня.
2	Представлення Даних		
3	Сеансовий	TCP, UDP	шлюз сеансового рівня.
4	Транспортний	TCP, UDP	
5	Мережевий	IP, ICMP	міжмережевий екран з фільтрацією пакетів.
6	Канальний	ARP, RAP	
7	Фізичний	Ethernet	

Як правило, чим вище рівень моделі OSI, на якому міжмережевий екран фільтрує пакети, тим вище рівень захисту, що забезпечується ним.

Міжмережеві екрани поділяють на чотири типи:

- міжмережеві екрани з фільтрацією пакетів;
- шлюзи транспортного і сеансового рівня;
- шлюзи прикладного рівня;
- міжмережеві екрани експертного рівня.

Відповідно, можна говорити про екрануючі концентратори (мости, комутатори) (рівень 2), маршрутизатори (рівень 3), про транспортне і сеансове екранування (рівень 4 і 5) і про прикладні

екрани (рівень 7). Існують також комплексні екрани (експертний рівень), що аналізують інформацію на декількох рівнях.

Фільтрація інформаційних потоків здійснюється міжмережевими екранами на основі набору правил, що є вираженням мережевих аспектів політики безпеки організації. У цих правилах, крім інформації, що міститься в фільтруючих потоках, можуть фігурувати дані, отримані з оточення, наприклад, поточний час, кількість активних сполук, порт, через який надійшов мережевий запит, і т.ін. Таким чином, у міжмережевих екранах використовується дуже потужний логічний підхід до розмежування доступу.

Можливості брандмауера безпосередньо визначаються тим, яка інформація може використовуватися в правилах фільтрації і яка може бути потужність наборів правил. Взагалі кажучи, чим вище рівень в моделі ISO/OSI, на якому функціонує МЕ, тим більше змістовна інформація йому доступна і, отже, тим тонше і надійніше він може бути налаштований.

Міжмережеві екрани з фільтрацією пакетів являють собою маршрутизатори або програми, що працюють на сервері та сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети. Тому такі екрани називають іноді пакетними фільтрами. Фільтрація здійснюється шляхом аналізу IP-адреси джерела і приймача, а також портів вхідних TCP- і UDP-пакетів і порівнянням їх з сконфігурованою таблицею правил. Рішення про те, пропустити або затримати дані, приймаються для кожного пакета незалежно, на підставі аналізу адрес і інших полів заголовків мережевого (канального) і, можливо, транспортного рівнів. Ще один важливий компонент, що аналізується – порт, через який надійшов пакет.

Екрануючі концентратори є не тільки засобом розмежування доступу, скільки оптимізації роботи локальної мережі за рахунок організації так званих віртуальних локальних мереж. Останні можна вважати важливим результатом застосування внутрішнього міжмережевого екранування.

Сучасні маршрутизатори дозволяють пов’язувати з кожним портом кілька десятків правил і фільтрувати пакети як на вході, так і на виході. В принципі, в якості пакетного фільтра може використовуватися і універсальний комп’ютер, обладнаний кількома мережевими картами.

Основні переваги екрануючих маршрутизаторів – доступна ціна (на межі мереж маршрутизатор потрібен практично завжди, питання лише в тому, як задіяти його екрануючі можливості) і прозорість для більш високих рівнів моделі OSI. Ці міжмережеві екрани прості у використанні і надають мінімальний вплив на продуктивність обчислювальної системи. Основний недолік – обмеженість інформації, що аналізується і, як наслідок, відносна слабкість захисту, вразливість при підміні адрес IP. Крім того, вони складні при конфігуруванні: для їх установки потрібне знання мережевих, транспортних і прикладних протоколів.

Транспортне екранування дозволяє контролювати процес встановлення віртуальних з’єднань і передачу інформації по ним. З точки зору реалізації екрануючий транспорт являє собою досить просту, а значить, надійну програму.

У порівнянні з пакетними фільтрами, транспортне екранування має більше інформації, тому відповідний МЕ може здійснювати більш тонкий контроль за віртуальними з’єднаннями (наприклад, він здатен відстежувати кількість переданої інформації і розривати з’єднання після перевищення певного порогу, перешкоджаючи тим самим несанкціонованому експорту інформації). Аналогічно, можливе накопичення більш змістовної реєстраційної інформації. Головний недолік – звуження сфери застосування, оскільки поза контролем залишаються датаграммні протоколи. Зазвичай транспортне екранування застосовують у поєднанні з іншими підходами, у якості важливого додаткового елементу.

Шлюзи сеансового рівня контролюють допустимість сеансу зв’язку. Вони стежать за підтвердженням зв’язку між авторизованим клієнтом і зовнішнім хостом (і навпаки), визначаючи, чи є запитуваний сеанс зв’язку допустимим. При

фільтрації пакетів шлюз сеансового рівня грунтується на інформації, що міститься у заголовках пакетів сеансового рівня протоколу TCP, тобто функціонує на два рівні вище, ніж міжмережевий екран з фільтрацією пакетів. Крім того, зазначені системи зазвичай мають функцію трансляції мережевих адрес, яка приховує внутрішні IP-адреси, тим самим, виключаючи підміну IP-адреси. Однак у таких міжмережевих екранах відсутній контроль вмісту пакетів, що генеруються різними службами. Для виключення зазначеного недоліку застосовуються шлюзи прикладного рівня.

Шлюзи прикладного рівня перевіряють вміст кожного пакета, що проходить через шлюз і можуть фільтрувати окремі види команд або інформації у протоколах прикладного рівня, які їм доручено обслуговувати. Це більш досконалий і надійний тип брандмауера, який використовує програми-посередники (proxies) прикладного рівня або агенти. Агенти складаються для конкретних служб мережі Інтернет (HTTP, FTP, Telnet тощо) і слугують для перевірки мережевих пакетів на наявність достовірних даних.

Міжмережевий екран, що функціонує на прикладному рівні, здатний забезпечити найбільш надійний захист. Як правило, подібний МЕ представляє собою універсальний комп'ютер, на якому функціонують екрануючі агенти, що інтерпретують протоколи прикладного рівня (HTTP, FTP, SMTP, telnet і т.ін.) в тій мірі, яка необхідна для забезпечення безпеки.

При використанні прикладних МЕ, крім фільтрації, реалізується ще один найважливіший аспект екранування. Суб'єкти з зовнішньої мережі бачать тільки шлюзовий комп'ютер і, відповідно, їм доступна тільки та інформація про внутрішні мережі, яку він вважає за потрібне експортувати. Прикладний МЕ насправді екранує, тобто закриває внутрішню мережу від зовнішнього світу. У той же час, суб'єктам внутрішньої мережі здається, що вони безпосередньо спілкуються з об'єктами зовнішнього світу. Недолік прикладних МЕ – відсутність повної прозорості, що вимагає спеціальних дій для підтримки кожного прикладного протоколу.

Якщо організація має в своєму розпорядженні початкові тексти прикладного МЕ і у змозі ці тексти модифікувати, перед нею відкриваються надзвичайно широкі можливості з налаштування екрану з урахуванням власних потреб. Справа в тому, що при розробці систем клієнт/сервер у багатоланковій архітектурі з'являються специфічні прикладні протоколи, які потребують захисту не менше стандартних. Підхід, заснований на використанні екрануючих агентів, дозволяє побудувати такий захист, не знижуючи безпеки та ефективності інших додатків і не ускладнюючи структуру зв'язків в міжмережевому екрані.

Міжмережеві екрани експертного рівня поєднують в собі елементи всіх трьох описаних вище категорій. Як і міжмережеві екрани з фільтрацією пакетів, вони працюють на мережевому рівні моделі OSI, фільтруючи вхідні і вихідні пакети на основі перевірки IP-адрес і номерів портів. Міжмережеві екрани експертного рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи належать пакети до відповідного сеансу. І, нарешті, брандмауери експертного рівня беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета відповідно до політики безпеки, виробленої в конкретній організації.

Замість застосування пов'язаних з додатками програм-посередників, брандмауери експертного рівня використовують спеціальні алгоритми розпізнавання та обробки даних на рівні додатків. За допомогою цих алгоритмів пакети порівнюються з відомими шаблонами даних, що теоретично повинно забезпечити більш ефективну фільтрацію пакетів.

Комплексні міжмережеві екрани, що охоплюють рівні від мережевого до прикладного, поєднують у собі кращі властивості «однорівневих» МЕ різних видів. Захисні функції виконуються комплексними МЕ прозорим для додатків чином, не вимагаючи внесення будь-яких змін ні в існуюче програмне забезпечення, ні в дії, що стали для користувачів звичними.

Комплексність МЕ може досягатися різними способами: «знизу вгору», від мережевого рівня через накопичення контексту

до прикладного рівня, або «зверху вниз», за допомогою доповнення прикладного МЕ механізмами транспортного і мережного рівнів.

Окрім наведених можливостей і визначеної кількості правил, якість брандмауера визначається ще двома дуже важливими характеристиками – простотою використання і власною захищеністю. У плані простоти використання першорядне значення мають наочний інтерфейс при визначенні правил фільтрації і можливість централізованого адміністрування складених конфігурацій.

У свою чергу, в останньому аспекті хотілося б виділити засоби централізованого завантаження правил фільтрації і перевірки набору правил на несуперечність. Важливим є і централізоване збирання і аналіз реєстраційної інформації, а також отримання сигналів про спроби виконання дій, заборонених політикою безпеки.

Власна захищеність брандмауера забезпечується тими ж засобами, що і захищеність універсальних систем. Мається на увазі фізичний захист, ідентифікація і аутентифікація, розмежування доступу, контроль цілісності, протоколювання і аудит. При виконанні централізованого адміністрування варто також подбати про захист інформації від пасивного і активного прослуховування мережі, тобто забезпечити її (інформації) цілісність і конфіденційність. Вкрай важливо оперативне накладення латок, які ліквідують виявлені вразливі місця МЕ.

Хотілося б підкреслити, що природа екранування як сервісу безпеки дуже глибока. Крім блокування потоків даних, що порушують політику безпеки, міжмережевий екран може приховувати інформацію про мережі, що захищаються, тим самим ускладнюючи дії потенційних зловмисників. Потужним методом приховування інформації є трансляція «внутрішніх» мережевих адрес, що попутно вирішує проблему розширення адресного простору, виділеного організації.

Відзначимо також наступні додаткові можливості міжмережевих екранів:

- контроль інформаційного наповнення (антивірусний контроль «з льоту», верифікація Java-аплетів, виявлення ключових слів в електронних повідомленнях тощо);
- виконання функцій ПЗ проміжного шару.

Особливо важливим є останній з перерахованих аспектів. ПЗ проміжного шару, як і традиційні міжмережеві екрани прикладного рівня, приховує інформацію про послуги, що надаються. За рахунок цього воно може виконувати такі функції, як маршрутизація запитів і балансування навантаження. Звісно ж цілком природним є бажання, щоб ці можливості були реалізовані в межах брандмауера. Це істотно спрощує дії щодо забезпечення високої доступності експортованих сервісів і дозволяє здійснювати перемикання на резервні потужності прозорим для зовнішніх користувачів чином. В результаті до послуг, що традиційно надаються міжмережевими екранами, додається підтримка високої доступності мережевих сервісів.

8.2.2. Тунелювання

Для передавання даних з достатнім ступенем захисту зазвичай створюються віртуальні канали між захищеними локальними мережами або комп'ютерами. Такий канал називається «тунелем», а технологія його створення називається «тунелюванням» або технологією віртуальних приватних мереж (VPN – Virtual Private Network). Вся інформація передається по тунелю у зашифрованому вигляді VPN-агентами.

У наш час тунелювання розглядається як самостійний сервіс безпеки. Його суть полягає в тому, щоб «упакувати» порцію даних, що передається разом зі службовими полями, у новий «конверт». В якості синонімів терміна «тунелювання» можуть використовуватися «конвертування» і «обгортання».

Тунелювання може застосовуватися для кількох цілей:

- передавання через мережу пакетів, що належать протоколу, який в даній мережі не підтримується (наприклад, передавання пакетів IPv6 через старі мережі, які підтримують тільки IPv4);
- забезпечення слабкої форми конфіденційності (в першу чергу конфіденційності трафіку) за рахунок приховування істинних адрес та іншої службової інформації;
- забезпечення конфіденційності і цілісності переданих даних при використанні разом з криптографічними сервісами.

Тунелювання може застосовуватися як на мережевому, так і на прикладному рівнях. Наприклад, стандартизовано тунелювання для IP і подвійне конвертування для пошти X.400.

На рис. 8.2.4 показаний приклад обгортання пакетів IPv6 у формат IPv4.

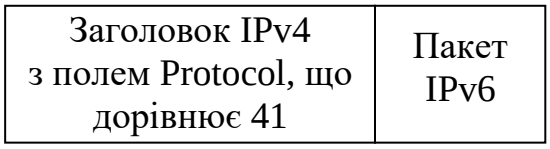


Рис. 8.2.4. Обгортання пакетів IPv6 в формат IPv4 з метою їх тунелювання через мережі IPv4

Комбінація тунелювання і шифрування (разом з необхідною криптографічного інфраструктурою) на виділених шлюзах і екранування на маршрутизаторах постачальників мережевих послуг (для розподілу просторів «своїх» і «чужих» мережевих адрес віртуальних локальних мереж) дозволяє реалізувати такий важливий в сучасних умовах захисний засіб, як віртуальні приватні мережі.

Технологія віртуальних приватних мереж (VPN – Virtual Private Network) є одним з ефективних механізмів забезпечення інформаційної безпеки при передаванні даних в розподілених обчислювальних мережах (рис. 8.2.5).

Віртуальні приватні мережі є комбінацією декількох самостійних сервісів (механізмів) безпеки:

• шифрування (з використання інфраструктури криптосистем) на виділених шлюзах (шлюз забезпечує обмін даними між обчислювальними мережами, що функціонують по різним протоколам);

• екранування (з використанням міжмережевих екранів);

• тунелювання.

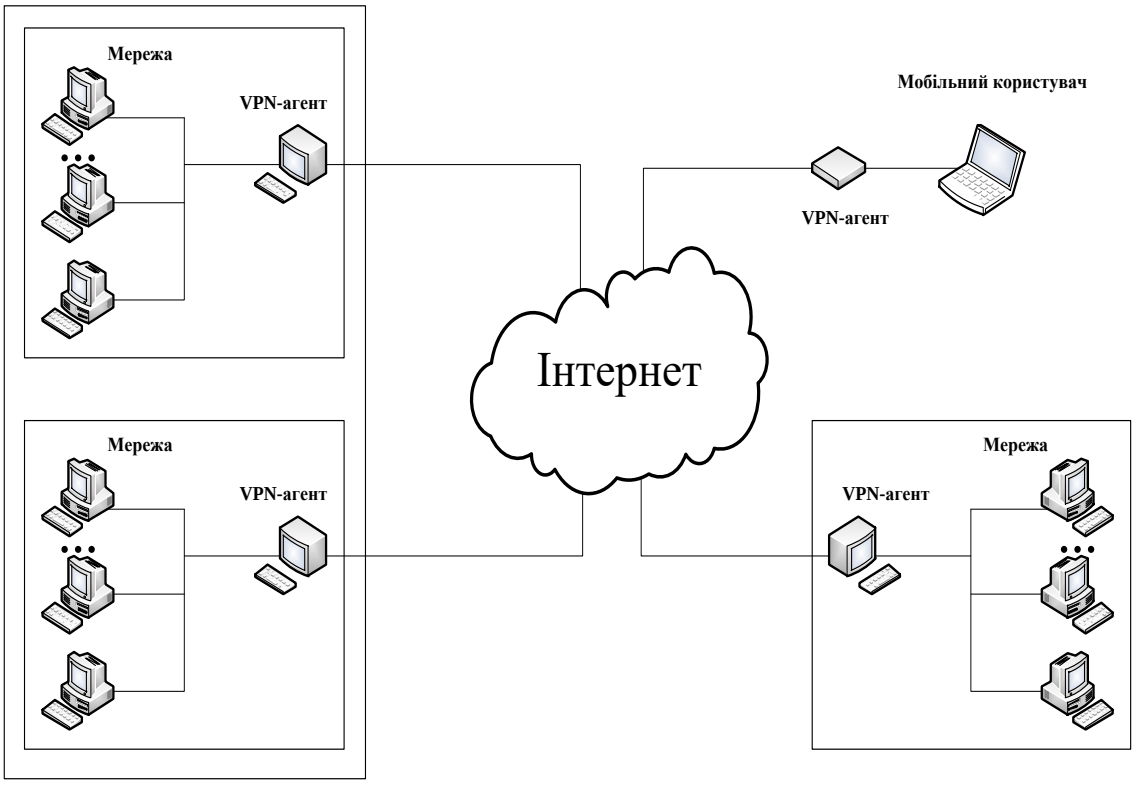


Рис. 8.2.5. Технологія віртуальних приватних мереж (VPN)

Сутність технології VPN полягає в наступному:

1. На всі комп'ютери, що мають вихід в Інтернет (або інша мережа загального користування), встановлюється VPN-агенти, які обробляють IP-пакети, що передаються по обчислювальних мережах.

2. Перед відправкою IP-пакету VPN-агент виконує наступні операції:

• аналізується IP-адреса одержувача пакета, в залежності від цієї адреси вибирається алгоритм захисту даного пакету (VPN-агенти можуть, підтримувати одночасно кілька алгоритмів

шифрування і контролю цілісності). Пакет може бути і зовсім відкинутий, якщо в налаштуваннях VPN-агента такий одержувач не значиться;

- обчислюється і додається в пакет його імітоприставка, що забезпечує контроль цілісності переданих даних;
- пакет шифрується (цілком, включаючи заголовок IP-пакета, що містить службову інформацію);
- формується новий заголовок пакета, де замість адреси одержувача вказується адреса його VPN-агента (ця процедура називається інкапсуляцією пакета).

В результаті цього обмін даними між двома локальними мережами зовні представляється як обмін між двома комп'ютерами, на яких встановлені VPN-агенти. Будь-яка корисна для зовнішньої атаки інформація, наприклад, внутрішні IP-адреси мережі, у цьому випадку недоступна.

3. При отриманні IP-пакета виконуються зворотні дії:

- із заголовка пакета отримується інформація про VPN-агента відправника пакета, якщо такий відправник не входить в число дозволених, то пакет відкидається (те ж саме відбувається при прийомі пакету з навмисно або випадково пошкодженим заголовком);
- згідно з налаштуваннями вибираються криптографічні алгоритми і ключі, після чого пакет розшифровується і перевіряється його цілісність (пакети з порушеною цілісністю також відкидаються);
- після всіх зворотних перетворень пакет в його початковому вигляді відправляється справжньому адресату по локальній мережі.

Всі перераховані операції виконуються автоматично, робота VPN-агентів є непомітною для користувачів. Складним є тільки налаштування VPN-агентів, що може бути виконане тільки дуже досвідченим користувачем. VPN-агент може знаходитися безпосередньо на комп'ютері, що захищається (це особливо корисно для мобільних користувачів). У цьому випадку він захищає

обмін даними тільки одного комп’ютера, на якому він встановлений.

Однією з обов’язкових функцій VPN-агентів є фільтрація пакетів. Фільтрація пакетів реалізується відповідно до VPN-агента, сукупність яких утворює політику безпеки віртуальної приватної мережі.

Для підвищення захищеності віртуальних приватних мереж на кінцях тунелів розташовуються міжмережеві екрани, які обслуговують підключення організацій до зовнішніх мереж (рис. 8.2.6). У такому випадку тунелювання і шифрування є додатковими перетвореннями, що виконуються в процесі фільтрації мережевого трафіку поряд з трансляцією адрес.

Кінцями тунелів, окрім корпоративних міжмережевих екранів, можуть бути мобільні комп’ютери співробітників (точніше, їх персональні МЕ).

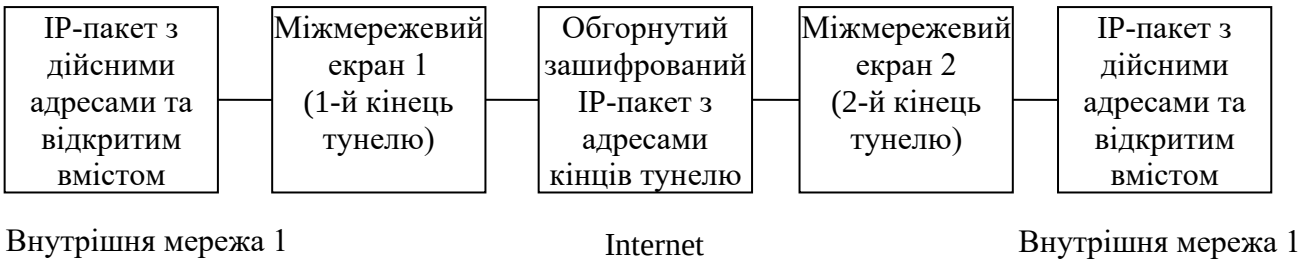


Рис. 8.2.6. Міжмережеві екрани як точки реалізації сервісу віртуальних приватних мереж

Подібні мережі, накладені зазвичай поверх Internet, істотно дешевші і набагато безпечніші, ніж власні мережі організації, побудовані на виділених каналах. Комунікації на всьому їх протязі фізично захистити неможливо, тому краще спочатку виходити з припущення про їх можливі вразливості і, відповідно, забезпечувати захист. Сучасні протоколи, спрямовані на підтримку класів обслуговування, допоможуть гарантувати для віртуальних приватних мереж задану пропускну здатність, величину затримок тощо, ліквідуючи тим самим єдину на сьогодні реальну перевагу власних мереж.

Тема 9. Аналіз захищеності, управління і забезпечення високої доступності

9.1. Аналіз захищеності

Сервіс аналізу захищеності призначений для виявлення вразливих місць з метою їх оперативної ліквідації. Сам по собі цей сервіс ні від чого не захищає, але допомагає виявити (і усунути) прогалини в захисті раніше, ніж їх зможе використовувати зловмисник. В першу чергу, маються на увазі не архітектурні (їх ліквідувати складно), а «оперативні» проломи, що з'явилися в результаті помилок адміністрування або через неуважність до оновлення версій програмного забезпечення.

Системи аналізу захищеності (сканери захищеності), як і розглянуті вище засоби активного аудиту, засновані на накопиченні і використанні знань. В даному випадку маються на увазі знання про прогалини в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати.

Відповідно, ядром таких систем є база вразливих місць, яка визначає доступний діапазон можливостей і вимагає практично постійної актуалізації.

В принципі, можуть виявлятися проломи самої різної природи: наявність шкідливого ПЗ (зокрема, вірусів), слабкі паролі користувачів, невдало сконфігуровані операційні системи, небезпечні мережеві сервіси, невстановлені латки, вразливості в додатках тощо. Однак найбільш ефективними є мережеві сканери (очевидно, в силу домінування сімейства протоколів TCP/IP), а також антивірусні засоби. При такому підході антивірусний захист можна зараховувати до засобів аналізу захищеності, не вважаючи його окремим сервісом безпеки.

Сканери можуть виявляти вразливі місця як шляхом пасивного аналізу, тобто вивчення конфігураційних файлів, задіяних портів тощо, так і шляхом імітації дій атакуючого. Прикладом може бути вільно розповсюджуваний сканер Nessus. Деякі знайдені вразливі місця можуть усуватися автоматично (наприклад, лікування заражених файлів), про інші повідомляється адміністратору.

Системи аналізу захищеності зазвичай забезпечені традиційними технологічними засобами – автовизначенням компонентів аналізованої ІС і графічним інтерфейсом, що допомагає, зокрема, ефективно працювати з протоколом сканування.

Контроль, що забезпечується системами аналізу захищеності, носить реактивний характер, він не захищає від нових атак, проте слід пам’ятати, що оборона повинна бути ешелонованою, і в якості одного з рубежів контроль захищеності цілком адекватний. Відзначимо також, що переважна більшість атак носить рутинний характер; вони можливі тільки тому, що відомі проломи в захисті роками залишаються неусуненими.

9.2. Управління

9.2.1. Основні поняття управління

Управління можна віднести до числа інфраструктурних сервісів, що забезпечують нормальну роботу компонентів і засобів безпеки. Складність сучасних систем така, що без правильно організованого управління вони поступово деградують як в плані ефективності, так і в плані захищеності.

Можливий і інший погляд на управління – як на інтегруючу оболонку інформаційних сервісів і сервісів безпеки (у тому числі засобів забезпечення високої доступності), що забезпечує їх

нормальне, узгоджене функціонування під контролем адміністратора ІС.

Відповідно до стандарту X.700, управління підрозділяється на:

- моніторинг компонентів;
- контроль (тобто видачу і реалізацію управляючих впливів);
- координацію роботи компонентів системи.

Системи управління повинні:

- дозволяти адміністраторам планувати, організовувати, контролювати і враховувати використання інформаційних сервісів;
- давати можливість відповідати на зміну вимог;
- забезпечувати передбачувану поведінку інформаційних сервісів;
- забезпечувати захист інформації.

Іншими словами, управління повинно мати досить високу функціональність, бути результативним, гнучким та інформаційно безпечним.

У X.700 виділяється п’ять функціональних областей управління:

- управління конфігурацією (установка параметрів для нормального функціонування, запуск і зупинка компонентів, збирання інформації про поточний стан системи, прийом повідомлень про суттєві зміни в умовах функціонування, зміна конфігурації системи);
- управління відмовами (виявлення відмов, їх ізоляція та відновлення працездатності системи);
- управління продуктивністю (збирання та аналіз статистичної інформації, визначення продуктивності системи у штатних і позаштатних умовах, зміна режиму роботи системи);
- управління безпекою (реалізація політики безпеки шляхом створення, видалення і зміни сервісів і механізмів безпеки, поширення відповідної інформації та реагування на інциденти);
- управління обліковою інформацією (тобто стягнення плати за користування ресурсами).

У стандартах сімейства X.700 описується модель управління, що здатна забезпечити досягнення поставлених цілей. Вводиться поняття керованого об'єкта як сукупності характеристик компонента системи, важливих з точки зору управління. До таких характеристик відносяться:

- атрибути об'єкта;
- допустимі операції;
- сповіщення, які об'єкт може генерувати;
- зв'язки з іншими керованими об'єктами.

Згідно з рекомендаціями X.701, системи управління розподіленими ІС будуються в архітектурі менеджер/агент. Агент (як програмна модель керованого об'єкта) виконує управляючі дії і породжує (при виникненні певних подій) сповіщення від його імені. У свою чергу, менеджер видає агентам команди на дії і отримує повідомлення.

Ієрархія взаємодіючих менеджерів і агентів може мати кілька рівнів. При цьому елементи проміжних рівнів грають двояку роль: по відношенню до вищих елементів вони є агентами, а до розташованих нижче – менеджерами. Багаторівнева архітектура менеджер/агент є ключем до розподіленого, масштабованого управління великими системами.

Логічно пов'язаною з багаторівневою архітектурою є концепція довіреного (або делегованого) управління. При довіреному управлінні менеджер проміжного рівня може управляти об'єктами, що використовують власні протоколи, в той час як «нагорі» спираються виключно на стандартні засоби.

Обов'язковим елементом при будь-якому числі архітектурних рівнів є управляюча консоль.

З точки зору вивчення можливостей систем управління слід враховувати розподіл, введений у X.701. У цьому документі управління підрозділяється на наступні аспекти:

- інформаційний (атрибути, операції і сповіщення керованих об'єктів);

- функціональний (управляючі дії і необхідна для них інформація);
- комунікаційний (обмін управляючою інформацією);
- організаційний (розбиття на області управління).

Ключову роль відіграє модель управляючої інформації. Вона описується рекомендаціями X.720. Модель є об'єктно-орієнтованою з підтримкою інкапсуляції і успадкування. Додатково вводиться поняття пакета як сукупності атрибутів, операцій, повідомлень і відповідної поведінки.

Клас об'єктів визначається позицією в дереві успадкування, набором включених пакетів і зовнішнім інтерфейсом, тобто видимими зовні атрибутами, операціями, повідомленнями і демонстрованою поведінкою.

До числа концептуально важливих можна віднести поняття «проактивного», тобто випереджаючого управління. Випереджаюче управління засноване на передбаченні поведінки системи на основі поточних даних і раніше накопиченої інформації. Найпростіший приклад подібного управління – видача сигналу про можливі проблеми з диском після серії помилок читання/запису, що нейтралізуються програмно. У більш складному випадку певний характер робочого навантаження і дій користувачів може передувати різкому уповільненню роботи системи; адекватним управляючим впливом могло б стати зниження пріоритетів деяких завдань і сповіщення адміністратора про наближення кризи.

9.2.2. Можливості типових систем управління

Розвинені системи управління мають двомірну налаштовуваність – на потреби конкретних організацій і на зміни в IT. Стандартні системи управління живуть (повинні жити) достатньо довго. За цей час в різних предметних галузях адміністрування (наприклад, в галузі резервного копіювання) напевно з'являться кращі рішення, ніж закладені спочатку в управляючий комплект, який повинен мати можливість (уміти)

еволюціонувати, причому різні його компоненти можуть робити це з різною швидкістю. Оскільки ніяка жорстка, монолітна система такого не витримає, єдиним виходом є наявність каркаса, з якого можна знімати старе і «навішувати» нове, не втрачаючи ефективності управління.

Каркас як самостійний продукт необхідний для досягнення принаймні наступних цілей:

- згладжування різнорідності керованих ІС, надання уніфікованих програмних інтерфейсів для швидкої розробки управляючих програм;
- створення інфраструктури управління, що забезпечує наявність таких властивостей, як підтримка розподілених конфігурацій, масштабованість, інформаційна безпека і т.ін.;
- надання функціонально корисних універсальних сервісів, таких як планування завдань, генерація звітів тощо.

Питання про те, що, крім каркаса, має входити в систему управління, є досить складним По-перше, багато систем управління мають мейнфреймове минуле і просто успадкували деяку функціональність, яка перестала бути необхідною. По-друге, для ряду функціональних завдань з’явилися окремі, високоякісні рішення, що перевершують аналогічні за призначенням «штатні» компоненти. Мабуть, з розвитком об’єктного підходу, багатоплатформності найважливіших сервісів і їх взаємної сумісності, системи управління дійсно перетворяться в каркас. Поки ж на їх частку залишається досить важливі області, а саме:

- управління безпекою;
- управління завантаженням;
- управління подіями;
- управління зберіганням даних;
- управління проблемними ситуаціями;
- генерація звітів.

На рівні інфраструктури є рішення ще одного найважливішого функціонального завдання – забезпечення автоматичного

виявлення керованих об’єктів, виявлення їх характеристик і зв’язків між ними.

Відзначимо, що управління безпекою в сукупності з відповідним програмним інтерфейсом дозволяє реалізувати платформно-незалежне розмежування доступу до об’єктів довільної природи і (що дуже важливо) винести функції безпеки з прикладних систем. Щоб з’ясувати, чи дозволений доступ поточною політикою для додатку, досить звернутися до менеджера безпеки системи управління.

Менеджер безпеки здійснює ідентифікацію/аутентифікацію користувачів, контроль доступу до ресурсів і протоколювання невдалих спроб доступу. Можна вважати, що менеджер безпеки вбудовується в ядро операційних систем контрольованих елементів ІС, перехоплює відповідні звернення і здійснює свої перевірки перед перевірками, що виконуються ОС, так що він створює ще один захисний кордон, не скасовуючи, а доповнюючи захист, який реалізовується засобами ОС.

Розвинені системи управління мають у своєму розпорядженні централізовану базу, в якій зберігається інформація про контрольовану ІС і, зокрема, деяке уявлення про політику безпеки. Можна вважати, що при кожній спробі доступу виконується перегляд збережених у базі правил, у результаті чого з’ясовується наявність у користувача необхідних прав. Тим самим для проведення єдиної політики безпеки в межах корпоративної інформаційної системи закладається міцний технологічний фундамент.

Зберігання параметрів безпеки в базі даних дає адміністраторам ще одну важливу перевагу – можливість виконання різноманітних запитів. Можна отримати список ресурсів, доступних даному користувачеві, список користувачів, що мають доступ до даного ресурсу і т. ін.

Одним з елементів забезпечення високої доступності даних є підсистема автоматичного управління зберіганням даних, що виконує резервне копіювання даних, а також автоматичне відстеження їх переміщення між основними і резервними носіями.

Для забезпечення високої доступності інформаційних сервісів використовується управління завантаженням, яке можна розподілити на управління проходженням завдань і контроль продуктивності.

Контроль продуктивності – поняття багатогранне. Сюди входять і оцінювання швидкодії комп'ютерів, і аналіз пропускної здатності мереж, і відстеження числа одночасно підтримуваних користувачів, і час реакції, і накопичення і аналіз статистики використання ресурсів. Зазвичай в розподіленій системі відповідні дані доступні «в принципі», вони поставляються точковими засобами управління, але проблема отримання цілісної картини, як поточної, так і перспективної, залишається досить складною. Вирішити її здатна система управління корпоративного рівня.

Засоби контролю продуктивності доцільно розбити на дві категорії:

- виявлення випадків неадекватного функціонування компонентів інформаційної системи і автоматичне реагування на ці події;
- аналіз тенденцій зміни продуктивності системи і довгострокове планування.

Для функціонування обох категорій засобів необхідно вибрати параметри які необхідно відслідковувати і допустимі межі для них, вихід за які означає «неадекватність функціонування». Після цього завдання зводиться до виявлення нетипової поведінки компонентів ІС, для чого можуть застосовуватися статистичні методи.

Управління подіями (точніше, повідомленнями про події) – це базовий механізм, що дозволяє контролювати стан інформаційних систем в реальному часі. Системи управління дозволяють класифікувати події і призначати для деяких з них спеціальні процедури обробки. Тим самим реалізується важливий принцип автоматичного реагування.

Очевидно, що завдання контролю продуктивності та управління подіями, так само як і методи їх вирішення в системах управління, близькі до аналогічних аспектів систем активного аудиту. У наявності ще одне свідчення концептуальної єдності

галузі знань під назвою «інформаційна безпека» і необхідності реалізації цієї єдності на практиці.

9.3. Доступність

9.3.1. Основні поняття доступності

Інформаційна система надає своїм користувачам певний набір послуг (сервісів). Вважається, що необхідний рівень доступності цих сервісів забезпечений, якщо такі показники знаходяться в заданих межах:

1. Ефективність послуги визначається в термінах загальної тривалості обслуговування запиту, кількості підтримуваних користувачів тощо. Потрібно, щоб ефективність не опускалася нижче заздалегідь встановленого рівня.

2. Час недоступності. Якщо ефективність інформаційної послуги не задовольняє накладеним обмеженням, послуга вважається недоступною. Потрібно, щоб максимальна тривалість періоду недоступності і сумарний час недоступності за деякий період (місяць, рік) не перевищували заздалегідь заданих меж.

По суті, потрібно, щоб інформаційна система майже завжди працювала з потрібною ефективністю. Для деяких критично важливих систем (наприклад, систем управління) час недоступності має бути нульовим, без всяких «майже». У такому випадку говорять про ймовірність виникнення ситуації недоступності і вимагають, щоб ця ймовірність не перевищувала заданої величини. Для вирішення даного завдання створювалися і створюються спеціальні відмовостійкі системи, вартість яких, як правило, досить висока.

До переважної більшості комерційних систем пред’являються менш жорсткі вимоги, однак сучасне ділове життя і тут накладає досить суворі обмеження, коли кількість обслуговуваних користувачів може вимірюватися тисячами, час відповіді не

повинен перевищувати декількох секунд, а час недоступності – кількох годин на рік.

Завдання забезпечення високої доступності необхідно вирішувати для сучасних конфігурацій, побудованих у технології клієнт/сервер. Це означає, що захисту потребує весь ланцюжок – від користувачів (можливо, віддалених) до критично важливих серверів (у тому числі серверів безпеки).

Основні загрози доступності були розглянуті нами раніше.

Відповідно до ГОСТ 27.002, під відмовою розуміється подія, яка полягає у порушенні працездатності виробу. У контексті даної роботи виріб – це інформаційна система або її компонент.

У найпростішому випадку можна вважати, що відмова будь-якого компонента складеного виробу ведуть до загальної відмови, а розподіл відмов у часі являє собою простий пуассоновский потік подій.

У такому випадку вводять поняття інтенсивності відмов і середнього часу напрацювання на відмову. У разі, якщо існує компонент, інтенсивність відмов якого багато більше, ніж у інших, то саме він визначає середній час напрацювання на відмову всієї ІС. Це є теоретичним обґрунтуванням принципу першочергового зміцнення найслабшої ланки.

Пуассонівська модель дозволяє обґрунтувати ще одне дуже важливе положення, яке полягає у тому, що емпіричний підхід до побудови систем високої доступності не може бути реалізований за прийнятний час. При традиційному циклі тестування/налагодження програмної системи за оптимістичними оцінками кожне виправлення помилки призводить до експоненціального зменшенням (приблизно на половину десяткового порядку) інтенсивності відмов. Відповідно, для того, щоб на досвіді переконатися у досягненні необхідного рівня доступності, незалежно від застосовуваної технології тестування і налагодження, доведеться витратити час, практично рівний середньому часу напрацювання на відмову. Наприклад, для досягнення середнього часу напрацювання на відмову 105 годин буде потрібно більше 104,5 годин, що становить більше трьох

років. Значить, потрібні інші методи побудови систем високої доступності, методи, ефективність яких доведена аналітично або практично за більш ніж п’ятдесят років розвитку обчислювальної техніки і програмування.

Пуассонівська модель може бути застосована у тих випадках, коли ІС містить поодинокі точки відмови, тобто компоненти, вихід з ладу яких веде до відмови всієї системи. Для дослідження систем з резервуванням застосовується інший формалізм. Відповідно до постановки завдання будемо вважати, що існує кількісна міра ефективності наданих виробом інформаційних послуг. У такому випадку вводяться поняття показників ефективності окремих елементів і ефективності функціонування всієї ІС.

В якості запобіжного заходу доступності можна прийняти ймовірність прийнятності ефективності послуг, що надаються інформаційною системою, на всьому протязі розглянутого відрізка часу. Чим більший запас ефективності є у розпорядженні системи, тим вище її доступність.

При наявності надмірності в конфігурації системи ймовірність того, що у даний проміжок часу ефективність інформаційних сервісів не опуститься нижче допустимої межі, залежить не тільки від імовірності відмови компонентів, але і від часу, протягом якого вони залишаються непрацездатними, оскільки при цьому сумарна ефективність падає, і кожна наступна відмова може стати фатальною. Щоб максимально збільшити доступність системи, необхідно мінімізувати час непрацездатності кожного компонента. Крім того, слід враховувати, що ремонтні роботи можуть викликати зниження ефективності або навіть тимчасового відключення працездатних компонентів і їх також необхідно мінімізувати.

Зазвичай у літературі з теорії надійності замість доступності говорять про готовність (у тому числі про високу готовність). На наш погляд термін «доступність» більше відображає сутність цього поняття. Він підкреслює, що інформаційний сервіс повинен бути не просто «готовий» сам по собі, але і доступний для своїх користувачів в умовах, коли ситуації недоступності можуть викликатися причинами, що на перший погляд не мають прямого

відношення до сервісу (приклад – відсутність консультаційного обслуговування).

Далі, замість часу недоступності зазвичай говорять про коефіцієнт готовності. Нам хотілося звернути увагу на два показники – тривалість одноразового простою і сумарну тривалість простоїв, тому ми вважали за краще використовувати термін «час недоступності» як більш ємний.

9.3.2. Основи заходів забезпечення високої доступності

Основою заходів підвищення доступності є застосування структурованого підходу, який знайшов втілення в об'єктно-орієнтованій методології. Структуризація необхідна по відношенню до всіх аспектів і складових частин інформаційної системи – від архітектури до адміністративних баз даних, на всіх етапах її життєвого циклу – від ініціації до виведення з експлуатації. Структуризація, що важлива сама по собі, є одночасно необхідною умовою практичної реалізованості інших заходів підвищення доступності. Тільки маленькі системи можна будувати і експлуатувати як завгодно. Великі системи мають свої закони, які, як ми вже вказували, програмісти вперше усвідомили більше 30 років тому.

При розробці заходів забезпечення високої доступності інформаційних сервісів рекомендується керуватися наступними архітектурними принципами, що розглядалися раніше:

- апробованість усіх процесів і складових частин інформаційної системи;
- уніфікація процесів і складових частин;
- керованість процесів, контроль стану частин;
- автоматизація процесів;
- модульність архітектури;
- орієнтація на простоту рішень.

Доступність системи у загальному випадку досягається за рахунок застосування трьох груп заходів, спрямованих на підвищення:

- безвідмовності (під цим розуміється мінімізація ймовірності виникнення будь-якого відмови; це елемент пасивної безпеки, який далі розглядатися не буде);
- відмовостійкості (здатності до нейтралізації відмов, «живучості», тобто здатність зберігати необхідну ефективність, незважаючи на відмови окремих компонентів);
- обслугованості (під обслугованістю розуміється мінімізація часу простою відмовили компонентів, а також негативного впливу ремонтних робіт на ефективність інформаційних сервісів, тобто швидке і безпечне відновлення після відмов).

Головне при розробці та реалізації заходів забезпечення високої доступності – повнота і систематичність. У зв'язку з цим вважаємо за доцільне скласти (і підтримувати в актуальному стані) карту інформаційної системи організації (на що ми вже звертали увагу), в якій фігурували б всі об'єкти ІС, їх стан, зв'язки між ними, процеси, асоційовані з об'єктами і зв'язками. За допомогою подібної карти зручно формулювати намічені заходи, контролювати їх виконання, аналізувати стан ІС.

9.3.3. Відмовостійкість і зона ризику

Інформаційну систему можна представити у вигляді графа сервісів, ребра в якому відповідають відношенню «сервіс А безпосередньо використовує сервіс В».

Нехай в результаті здійснення певної атаки (джерелом якої може бути як людина, так і явище природи) виводиться з ладу підмножина сервісів S_1 (тобто ці сервіси в результаті нанесених ушкоджень стають непрацездатними). Назвемо S_1 зоною ураження.

У зону ризику S ми будемо включати всі сервіси, ефективність яких при здійсненні атаки падає нижче допустимої межі. Очевидно, S_1 – підмножина S. S строго включає S_1, коли є сервіси,

безпосередньо не порушені атакою, але критично залежні від уражених, тобто нездатні переключитися на використання еквівалентних послуг або в силу відсутності таких, або в силу неможливості доступу до них. Наприклад, зона ураження може зводитися до одного порту концентратора, обслуговуючого критичний сервер, а зона ризику охоплює всі робочі місця користувачів сервера.

Щоб система не містила одиночних точок відмови, тобто залишалася «живучою» при реалізації будь-якої з розглянутих загроз, жодна зона ризику не повинна включати в себе послуги, що надаються. Нейтралізацію відмов потрібно виконувати всередині системи, непомітно для користувачів, за рахунок розміщення достатньої кількості надлишкових ресурсів.

З іншого боку, природно порівнювати зусилля щодо забезпечення «живучості» з розглянутими загрозами. Коли розглядається набір загроз, відповідні їм зони ураження можуть виявитися вкладеними, так що «живучість» по відношенню до більш серйозних загроз автоматично тягне за собою і «живучість» у більш легких випадках.

Слід враховувати, що зазвичай вартість перемикання на резервні ресурси зростає разом зі збільшенням обсягу цих ресурсів. Значить, для найбільш ймовірних загроз доцільно мінімізувати зону ризику, навіть якщо передбачена нейтралізація яка охоплює загрози. Немає сенсу перемикатися на резервний обчислювальний центр тільки тому, що у одного з серверів вийшов з ладу блок живлення.

Зону ризику можна трактувати не тільки як сукупність ресурсів, а й як частину простору, яка зачіпається при реалізації загрози. У такому випадку, як правило, чим більше відстань дублюючого ресурсу від меж зони ризику, тим вище вартість його підтримки, оскільки збільшується протяжність ліній зв’язку, час перекидання персоналу і т.ін. Це є ще одним аргументом на користь адекватної протидії загрозам, які слід брати до уваги при розміщенні надлишкових ресурсів і, зокрема, при організації резервних центрів.

Введемо ще одне поняття. Назвемо зоною нейтралізації загрози сукупність ресурсів, залучених у нейтралізацію відмови, яка виникла внаслідок реалізації загрози. Маються на увазі ресурси, режим роботи яких у разі відмови змінюється. Очевидно, зона ризику є підмножиною зони нейтралізації. Чим менше різниця між ними, тим економічніше діє цей механізм нейтралізації.

Все, що знаходиться поза зоною нейтралізації, відмови «не відчуває» і може трактувати внутрішність цієї зони як безвідмовну. Таким чином, в ієрархічно організованій системі грань між «живучістю» і обслуговуваністю, з одного боку, і безвідмовністю, з іншого боку, відносна. Доцільно конструювати цілісну інформаційну систему з компонентів, які на верхньому рівні можна вважати безвідмовними, а питання «живучості» і обслуговуваності вирішувати в межах кожного компонента.

9.3.4. Забезпечення відмовостійкості

Основним засобом підвищення «живучості» є внесення надмірності в конфігурацію апаратних і програмних засобів, що підтримує інфраструктуру та персонал, резервування технічних засобів і тиражування інформаційних ресурсів (програм і даних).

Заходи щодо забезпечення відмовостійкості можна розділити на локальні і розподілені. Локальні заходи спрямовані на досягнення «живучості» окремих комп'ютерних систем або їх апаратних і програмних компонентів (в першу чергу з метою нейтралізації внутрішніх відмов ІС). Типові приклади подібних заходів – використання кластерних конфігурацій в якості платформи критичних серверів або «гаряче» резервування активного мережного обладнання з автоматичним перемиканням на резерв.

Якщо в число розглянутих ризиків входять серйозні аварії підтримуючої інфраструктури, що призводять до виходу з ладу виробничого майданчика організації, слід передбачити розподілені заходи забезпечення живучості, такі як створення або оренда

резервного обчислювального центру. При цьому, крім дублювання і/або тиражування ресурсів, необхідно передбачити засоби автоматичного або швидкого ручного переконфігуруванні компонентів ІС, щоб забезпечити перемикання з основного майданчика на резервний.

Апаратура – відносно статична складова, проте було б помилкою повністю відмовляти їй у динамічності. У більшості організацій інформаційні системи знаходяться в постійному розвитку, тому протягом усього життєвого циклу ІС слід співвідносити всі зміни з необхідністю забезпечення «живучості», не забувати «тиражувати» нові і модифіковані компоненти.

Програми та дані динамічніші, ніж апаратура, і резервуватися вони можуть постійно, при кожній зміні, після завершення певної логічно замкнутої групи змін або після закінчення певного часу.

Резервування програм і даних може виконуватися багатьма способами – за рахунок зеркалювання дисків, резервного копіювання та відновлення, реплікації баз даних і т. ін. Будемо використовувати для всіх перерахованих способів термін «тиражування».

Виділимо наступні класи тиражування:

- Симетричне/асиметричне. Тиражування називається симетричним, якщо всі сервери, що надають цей сервіс, можуть змінювати належну їм інформацію і передавати зміни інших серверів. В іншому випадку тиражування називається асиметричним.
- Синхронне/асинхронне. Тиражування називається синхронним, якщо зміна передається всім екземплярам сервісу в межах однієї розподіленої транзакції. В іншому випадку тиражування називається асинхронним.
- Здійснюване засобами сервісу, що зберігає інформацію зовнішніми засобами.

Розглянемо, які методи тиражування є кращими.

Безумовно, слід віддати перевагу стандартним засобам тиражування, вбудованим у сервіс.

Асиметричне тиражування теоретично простіше симетричного, тому доцільно вибрати асиметрію.

Найважче вибрати між синхронним і асинхронним тиражуванням. Синхронне ідейно простіше, але його реалізація може бути великоваговою і складною, хоча це внутрішня складність сервісу, що невидима для додатків. Асинхронне тиражування стійкіше до відмов в мережі, і воно менше впливає на роботу основного сервісу.

Чим надійніше зв'язок між серверами, залученими в процес тиражування, чим менше час, що відводиться на перемикання з основного сервера на резервний, чим жорсткіше вимоги до актуальності інформації, тим кращим виявляється синхронне тиражування.

З іншого боку, недоліки асинхронного тиражування можуть компенсуватися процедурними і програмними заходами, спрямованими на контроль цілісності інформації в розподіленій ІС. Сервіси, що входять до складу ІС, у змозі забезпечити ведення і зберігання журналів транзакцій, за допомогою яких можна виявляти операції, загублені при перемиканні на резервний сервер. Навіть в умовах нестійкого зв'язку з віддаленими філіями організації подібна перевірка у фоновому режимі займе не більше декількох годин, тому асинхронне тиражування може використовуватися практично у будь-якій ІС.

Асинхронне тиражування може проводитися на сервері, що працює в режимі «гарячого» резерву, можливо, навіть обслуговуючого частину призначених для користувача запитів, або на сервері, що працює в режимі «теплого» резерву, коли зміни періодично «накочуються», але сам резервний сервер запитів не обслуговує.

Перевага «теплого» резервування полягає в тому, що його можна реалізувати, надаючи менший вплив на основний сервер. Цей вплив взагалі може бути зведений до нуля, якщо асинхронне тиражування здійснюється шляхом передавання інкрементальних копій з основного сервера (резервне копіювання необхідно виконувати у будь-якому випадку).

Основний недолік «теплого» резерву складається в тривалому часі включення, що може бути неприйнятним для «важких» серверів, таких як кластерна конфігурація сервера СУБД. Тут необхідно проводити вимірювання в умовах, близьких до реальних.

Інший недолік «теплого» резерву випливає з небезпеки малих змін. Може виявитися, що в найпотрібніший момент терміновий переклад резерву в штатний режим неможливий.

З огляду на наведені міркування, слід в першу чергу розглядати можливість «гарячого» резервування, або ретельно контролювати використання «теплого» резерву і регулярно (не рідше одного разу на тиждень) проводити пробні перемикання резерву в «гарячий» режим.

9.3.5. Програмне забезпечення проміжного шару

За допомогою програмного забезпечення проміжного шару (ПЗ ПШ) можна для довільних прикладних сервісів домогтися високої «живучості» з повністю прозорим для користувачів перемиканням на резервні потужності.

Перерахуємо основні переваги ПЗ ПШ, істотні для забезпечення високої доступності.

- ПЗ ПШ зменшує складність створення розподілених систем. Подібне ПЗ бере на себе частину функцій, які в локальному випадку виконують ОС;
- ПЗ ПШ бере на себе маршрутизацію запитів, дозволяючи тим самим забезпечити «живучість» прозорим для користувачів чином;
- ПЗ ПШ здійснює балансування завантаження обчислювальних потужностей, що також сприяє підвищенню доступності даних;
- ПЗ ПШ у змозі здійснювати тиражування будь-якої інформації, а не тільки вмісту баз даних. Отже, будь-який додаток можна зробити стійким до відмов серверів;
- ПЗ ПШ в змозі відслідковувати стан додатків і при необхідності тиражувати і перезапускати програми, що гарантує «живучість» програмних систем;

• ПЗ ПШ дає можливість прозорим для користувачів чином виконувати переконфігурування (і, зокрема, нарощування) серверних компонентів, що дозволяє масштабувати систему, зберігаючи інвестиції у прикладні системи. Стабільність прикладних систем – важливий фактор підвищення доступності даних.

Раніше ми згадували про переваги використання ПЗ ПШ в межах міжмережевих екранів, які в такому випадку стають елементом забезпечення відмовостійкості інформаційних сервісів.

9.3.6. Забезпечення обслуговуваності

Заходи щодо забезпечення обслуговуваності спрямовані на зниження термінів діагностування та усунення відмов і їх наслідків.

Для забезпечення обслуговуваності рекомендується дотримуватися таких архітектурних принципів:

• орієнтація на побудову інформаційної системи з уніфікованих компонентів з метою спрощення заміни відмовили частин;

• орієнтація на модульну структуру з можливістю автоматичного виявлення відмов, динамічного переконфігурування апаратних і програмних засобів і заміни компонентів, що відмовили, в «гарячому» режимі.

Динамічне переконфігуруванні має дві основні цілі:

• ізоляція відмовили компонентів;

• збереження працездатності сервісів.

Ізольовані компоненти утворюють зону ураження реалізованої загрози. Чим менше відповідна зона ризику, тим вище обслуговуваність сервісів. Так, при відмовах блоків живлення, вентиляторів і/або дисків у сучасних серверах зона ризику обмежується відмовленим компонентом; при відмовах процесорних модулів весь сервер може зажадати перезавантаження (що може викликати подальше розширення зони ризику). Очевидно, в ідеальному випадку, зони ураження і ризику збігаються, і сучасні

сервери і активне мережеве обладнання, а також програмне забезпечення провідних виробників дуже близькі до цього ідеалу.

Можливість програмування реакції на відмову також підвищує обслуговуваність систем. Кожна організація може вибрати свою стратегію реагування на відмови тих чи інших апаратних і програмних компонентів і автоматизувати цю реакцію. Так, в найпростішому випадку можлива відправка повідомлення системного адміністратора, щоб прискорити початок ремонтних робіт. У більш складному випадку може бути реалізована процедура «м'якого» виключення (перемикання) сервісу, щоб спростити обслуговування.

Можливість віддаленого виконання адміністративних дій – важливий напрямок підвищення обслуговуваності, оскільки при цьому прискорюється початок відновлювальних заходів, а в ідеалі всі роботи (зазвичай пов'язані з обслуговуванням програмних компонентів) виконуються у віддаленому режимі, без переміщення кваліфікованого персоналу, тобто з високою якістю і у найкоротші терміни. Для сучасних систем можливість віддаленого адміністрування – стандартна властивість, але важливо дбати про її практичну можливість бути реалізованою в умовах різнорідності конфігурацій (в першу чергу клієнтських). Централізоване поширення і конфігурація програмного забезпечення, управління компонентами інформаційної системи і діагностування – надійний фундамент технічних заходів підвищення обслуговуваності.

Істотний аспект підвищення обслуговуваності – організація консультаційної служби для користувачів (обслуговуваність користувачів), впровадження програмних систем для роботи цієї служби, забезпечення достатньої пропускної здатності каналів зв'язку з користувачами, у тому числі в режимі пікових навантажень.

Розділ III

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ОРГАНІЗАЦІЙНО-ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

Тема 10. Нормативні акти про інформаційну безпеку та захист інформації

10.1. Технічний захист інформації (ТЗІ): поняття, концепція, стан, напрямки державної політики

ТЗІ (Технічний захист інформації) – це сукупність організаційних структур, поєднаних цілями захисту інформації, нормативно-правової та матеріально-технічної бази і спрямована на забезпечення інженерно-технічними засобами конфіденційності, цілісності та доступності інформації. Органом ТЗІ є Департамент спеціальних систем та захисту інформації СБУ. ТЗІ відбувається відповідно до «Положення про ТЗІ в Україні», затвердженого Указом Президента 1999 р.

Концепція ТЗІ в Україні затверджена Постановою КМУ 8 жовтня 1997 року. Концепція визначає основи державної політики у сфері ТЗІ.

ТЗІ – це діяльність, спрямована на забезпечення інженерно-технічними засобами порядку доступу, цілісності та доступності інформації, яка становить державну та іншу таємницю, конфіденційну інформацію, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства та держави. Витік інформації, яка становить ДТ, або іншу таємницю, конфіденційну інформацію – одна із загроз національній безпеці України в інформаційній сфері.

Загрози інформаційній безпеці зумовлені:

- неефективністю державної політики в галузі ІТ;
- діяльністю іноземних держав;
- діяльністю політичних партій та окремих осіб у політичній боротьбі та конкуренції;
- злочинною діяльністю, спрямованою на протизаконне отримання інформації;
- використанням технологій низької якості;
- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, низькою кваліфікацією кадрів у ТЗІ.

Стан ТЗІ в Україні зумовлюється:

- недосконалістю правового регулювання інформаційної сфери, зокрема, захисту таємниць, конфіденційної інформації;
- недостатністю правових актів з питань досліджень ТЗІ;
- незавершеністю сертифікації ТЗІ;
- неузгодженістю правових актів ТЗІ з міжнародними угодами.

Правову основу ТЗІ складають: Конституція України, Концепція національної безпеки, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію».

Основні напрямки державної політики у сфері ТЗІ:

- нормативно-правове забезпечення;
- розробка нормативних актів захисту важливої відкритої інформації;
- організація забезпечення ТЗІ;

- контроль за імпортом технологій ТЗІ;
- підготовка кадрів у галузі ТЗІ;
- розвиток міжнародної співпраці у сфері ТЗІ.

До державних стандартів і нормативних документів, що стосуються технічного захисту інформації (ТЗІ) відносяться такі документи: «Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення» (ДСТУ 3396.0-96); Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт» (ДСТУ 3396.1-96); «Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення“ (ДСТУ 3396.2-96).

Ці стандарти установлюють об’єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов’язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб’єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють та користуються інформацією, що підлягає технічному захисту.

Об’єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження. Об’єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ. Цими стандартами визначаються носії ІзОД, середовище поширення, мета ТЗІ (див. далі), джерела загроз.

До джерел загроз відносяться діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Далі

йдеться про канали поширення загроз, розроблення і реалізацію системи захисту інформації, контроль за ТЗІ та функції нормативних документів у сфері ТЗІ. До таких функцій, зокрема, належить: проведення єдиної технічної політики; створення і розвиток єдиної термінологічної системи; функціонування багаторівневих систем захисту інформації на основі взаємопогоджених положень, правил, методик, вимог та норм; функціонування систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації; розвиток сфери послуг у галузі ТЗІ; установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апаратури; організація проектування будівельних робіт у частині забезпечення ТЗІ; підготовка та перепідготовка кадрів у системі ТЗІ. Нормативні документи системи ТЗІ поділяються на: нормативні документи із стандартизації у галузі ТЗІ; державні стандарти та прирівняні до них нормативні документи; нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України; нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом; нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

10.2. Захист інформації в автоматизованих системах

Широке впровадження інформаційних технологій у сфері державної діяльності, економіки, фінансів зумовило підвищення вимог до забезпечення безпеки інформації в АС. Особливо гостро це питання стоїть у контексті появи «комп'ютерних злочинів». З цією метою 1994 року прийнято Закон України «Про захист інформації в АС».

Карний Кодекс України (ст. 1981) здійснює кримінально-правову охорону інформації в АС. Встановлюється відповідальність за наступні форми злочинів:

1. Умисне втручання в роботу АС, що призвело до перекручення чи знищення інформації.

2. Поширення програмних і технічних засобів, призначених для незаконного проникнення в АС і здатних призвести до перекручення та знищення інформації.

Таке вузьке коло злочинних дій вказує на необхідність термінового реформування кримінального законодавства. Фахівці рекомендують внести до кримінального кодексу цілу низку статей, які відображають нові способи здійснення комп'ютерних злочинів. Зокрема, це такі статті, як:

- розповсюдження технічних засобів, призначених для отримання несанкціонованого доступу до комп'ютерів, АС і мереж;
- навмисне знищення, блокування та модифікація комп'ютерної інформації, що призвело до тяжких наслідків;
- навмисне знищення ІзОД;
- навмисне порушення режиму доступу до комп'ютерної інформації з ОД, яке призвело до витоку, знищення, модифікації інформації;
- порушення правил функціонування АС;
- навмисне порушення права уповноваженої особи на використання ресурсів комп'ютера;
- злочинне недбальство.

На думку правників, повинно бути законодавчо встановлене обмеження вільного обігу програмно-технічних засобів несанкціонованого доступу. Особа має нести кримінальну або адміністративну відповідальність залежно від тяжкості злочину. Об'єктом злочину повинно бути право власності на інформацію, тобто порушення права власника на володіння, використання комп'ютерної інформації.

Основні положення Закону України «Про захист інформації в АС».

АС – це система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки, а також методи і процедури, програмне забезпечення.

Інформація в АС – це сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення.

Захист інформації в АС – це сукупність організаційно-технічних заходів і правових норм для запобігання шкоди інтересам власників інформації. Закон визначає й інші терміни: «обробка інформації», «несанкціонований доступ», «розпорядник АС», «персонал АС», «користувач АС», «витік інформації», «підробка інформації», «блокування інформації» та ін.

Об'єктами захисту закону є інформація, що обробляється в АС, права власників інформації, права користувача. Суб'єктами відносин закон визнає власників інформації або їхніх уповноважених осіб, власників АС та їхніх представників, користувачів інформації, користувачів АС.

За ст. 4 право власності на інформацію встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АС. Якщо угоди немає, така інформація належить користувачу АС, який здійснив обробку. Користувач може обробляти інформацію лише за згодою власника, якщо це загальнодоступна інформація.

За ст.7, яка регулює відносини між власником інформації та власником АС, власник АС повинен забезпечити захист інформації згідно угоди з власником інформації. Якщо інформація належить до ДТ, її захист здійснюється згідно з рішенням уповноваженого КМУ. Власник АС не відповідає за шкоду, завдану інформації, якщо при цьому не було порушено встановлених власником інформації правила її захисту.

Захист інформації в АС здійснюється шляхом:

- дотримання суб'єктами правових відносин, норм, вимог та правил організаційно-технічного характеру щодо захисту інформації;
- перевірки відповідності засобів АС встановленим вимогам ЗІ.

Інформація, що є власністю держави, повинна оброблятися в АС, що має відповідний сертифікат захищеності і визначається уповноваженим КМУ. Закон встановлює відповідальність за порушення порядку і правил ЗІ, механізм відшкодування нанесеної шкоди, гарантує забезпечення інформаційних прав України.

10.3. Інтернет як об'єкт інформаційного права та ІБ

Інтернет з'явився великою мірою спонтанно. Його витоки сягають епохи «холодної війни». Вперше Інтернет виник у Пентагоні 1969 року і мав назву Arpa net (Агентство передових досліджень проектів Пентагона). До початку 80-х років XX ст. пентагонівський Інтернет складався з 500 комп'ютерів у військових лабораторіях та університетах. Із розростанням мережі, збільшенням обсягу інформації у системі, почали з'являтися питання правового характеру, пов'язані, насамперед, з тим, що Інтернет – інтернаціональна мережа, що не знає кордонів. Тому є потреба розробляти юридичний статус Інтернету на рівні міжнародного законодавства.

Отже, що таке Інтернет з юридичної точки зору? Є дві відповіді на це питання: з одного боку, Інтернет – це таке середовище, до якого право принципово не застосовується; з другого боку, можливе правове регулювання інтернет-стосунків. Виникає у цьому зв'язку і питання, чи є Інтернет суб'єктом права? Адже Інтернет не є ані міжнародною організацією, ні державним закладом, ні юридичною особою, ні громадським об'єднанням, тому Інтернет в цілому не може бути суб'єктом права. Чи є Інтернет об'єктом права? Устаткування, засоби зв'язку та комунікацій, з яких складається Інтернет, не мають конкретного власника. Відтак, Інтернет не є і об'єктом права.

Такі висновки дають підстави порівнювати Інтернет зі звичайним матеріальним середовищем, тобто з реальним життям. Ми здійснюємо в Інтернеті ті самі дії, що і в реальному житті.

Тому, Інтернет – це сфера нашого побутового життя, правда віртуального. Особливість регулювання інформаційних відносин в Інтернеті визначається особливістю фізичного представлення інформації в мережі, в першу чергу, в електронному вигляді.

При передачі інформації відсутній носій інформації, що ускладнює оформлення і представлення документованої інформації у віртуальному середовищі, передусім офіційних документів. Виникає проблема закріплення і захисту правового режиму електронного документа, який би гарантував достовірність та оригінальність. Відтак, актуальною є проблема електронного підпису. Це дає можливість створювати документи, достовірність яких буде ще гарантованішою, ніж у звичайних документах.

В Інтернеті діють три групи суб'єктів:

1) ті, що створюють програмно-технічну частину інформаційної інфраструктури;

2) суб'єкти, що виробляють і поширюють інформацію в Інтернеті, підключають до мережі;

3) споживачі-користувачі інформації Інтернету.

Отже, об'єктами, з приводу яких виникають інформаційні відносини в Інтернеті є:

- програмно-технічні комплекси, інформаційні системи;
- інформація, інформаційні ресурси;
- доменне ім'я;
- інформаційні права та свободи;
- інтереси особистості, суспільства та держави;
- інформаційний суверенітет держави;
- інформаційна безпека.

Виникають проблеми, пов'язані з поширенням електронних документів:

- визначення поняття "електронний документ";
- підтвердження юридичної сили електронного документа;
- встановлення факту і дати введення документа в мережу;
- ідентифікація змісту електронного документа з його власником;

- доведення права авторства електронного документа.

З позицій інформаційної безпеки Інтернет може використовуватися зі злочинною метою:

- злочини проти мережі і системи обробки інформації (несанкціонований доступ до інформаційних ресурсів);
- злочини «вираження думки» (насильство, порнографія, незаконна реклама).

Таким чином, ІБ в Інтернеті спрямована на захист:

- національної безпеки (виробництво наркотиків, зброї, терористична діяльність тощо);
- неповнолітніх;
- людської гідності;
- інформації (несанкціонований доступ);
- таємниці особистого життя;
- репутації;
- інтелектуальної власності (незаконне поширення творів, програмного забезпечення, музики тощо).

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія / Д. С. Азаров. – К. : Атіка, 2007. – 304 с.
2. Англо-украинско-русский словарь с толкованиями по безопасности информации в компьютерных системах : Около 1100 терминов. – К. : КМУГА, 1997. – 200 с.
3. Антонов В. М. Інтелектуальна власність і комп'ютерне авторське право / В. М. Антонов. – К. : КНТ, 2005. – 520 с.
4. Антонюк А. О., Жора В. В. Теоретичні основи моделювання та аналізу систем захисту інформації : [монографія] / А. О. Антонюк, В. В. Жора. – Ірпінь : Національний університет ДПС України, 2010. – 310 с.
5. Антонюк А. О. Захист від комп'ютерних вірусів : навчальний посібник / А. О. Антонюк, Л. В. Дубчак, В. Ю. Свириденко. – Ірпінь : Національний університет ДПС України, 2008. – 285 с.
6. Архипов О. Є., Бородавко І. Т., Ворожко В. П. Оцінювання ефективності системи охорони державної таємниці : монографія / О. Є. Архипов, І. Т. Бородавко, В. П. Ворожко. – К. : Наук.-вид. відділ НА СБ України, 2007. – 63 с.
7. Атаки на відмову в мережі Інтернет: опис проблеми та підходів щодо її вирішення / П. І. Андон, О. П. Ігнатенко. – Київ, 2008. – 50 с. – (Препр. / НАН України. Ін-т програмних систем; 2008-2).
8. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М. : Бином-Пресс, 2002 г. – 384 с.
9. Біленчук П. Д. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-іфіміналісти : монографія / П. Д. Біленчук, М. В. Гуцалюк, О. В. Кравчук, М. В. Козир ; за заг. ред. П. Д. Біленчука. – К. : Наука і життя, 2008. – 291 с.
10. Біленчук П. Д. Комп'ютерний тероризм : практика запобігання, протидії, розслідування : навчальний посібник / П. Д. Біленчук , В. В. Кравчук, О. В. Кравчук, В. М. Кулик ; за заг. ред. П. Д. Біленчука. – Хмельницький : Хм. ЦНТЕІ, 2008. – 258 с.
11. Боротьба в інформаційних війнах та інформаційне право : монографія ; за ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. – К. : НДЦПІ АПрН України, 2007 р. – 234 с.

12. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.

13. Брижко В. М., Базанов Ю. К., Харченко Л. С. Ліцензування прав на інформаційні ресурси / В. М. Брижко, Ю. К. Базанов, Л. С. Харченко. – К. : Національне агентство з питань інформатізації при Президентові України, 1997 р.

14. Васильцов І. В. Атаки спеціального виду на криптопристрої та методи боротьби з ними / І. В. Васильцов ; за науковою редакцією д. т. н., проф. В. П. Широчина. – Кременець : Видавничий центр КОГПІ, 2009. – 264 с.

15. Вертузаєв М. С. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посібник / М. С. Вертузаєв, О. М. Юрченко ; за ред. С. Г. Лаптєва. – К. : Вид-во Європ. ун-ту, 2001. – 321 с.

16. Вильям Столлингс. Основы защиты сетей. Приложения и стандарты : пер. с англ. / Вильям Столлингс. – М. : Издательский дом «Вильямс», 2002. – 432 с.

17. Вишняков В. М. Захист даних в інформаційних системах : навчальний посібник / В. М. Вишняков. – К. : КНУБА, 2010. – 128 с.

18. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій : наук.-практ. посіб. / Б. В. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов ; за заг. ред. проф. Я. Ю. Кондратьева. – К. : Вид. ПАЛИВОДА А. В., 2004. – 144 с.

19. Гайворонський М. В., Новиков О. М. Безпека інформаційно-комунікаційних систем / Гайворонський М. В., О. М. Новиков. – К. : Видавнича група BHV, 2009. – 608 с.

20. Головань С. М. Інтелектуальна власність у сфері захисту інформації / С. М. Головань, С. Р. Коженевський, О. І. Стельмаховська, В. О. Хорошко ; за ред. проф. В. О. Хорошка. – К. : ДУІКТ, 2009. – 177 с.

21. Голубев В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека : проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубев, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. доктора юридичних наук, професора Р. А. Калюжного. – Запоріжжя : Просвіта, 2001. – 252 с.

22. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посібник / В. О. Голубев, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. доктора юридичних наук, професора Р. А. Калюжного. – Запоріжжя : ГУ ЗІДМУ'/ 2002. – 292 с.

23. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003 – 250 с.
24. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
25. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
26. Державна та комерційна таємниця. Нормативно-правове регулювання / О. М. Роїна. – К. : КНТ, 2006. – 424 с.
27. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року // www.iu.org.ua
28. Дмитришин В. С. Інтелектуальна власність на програмне забезпечення в Україні / В. С. Дмитришин, В. І. Березанська. – К. : Вірлен, 2005. – 304 с.
29. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : Издательство «Диа- Софт», 1999. – 480 с.
30. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО «ТИД «ДС», 2004. – 992 с.
31. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К. : ООО «ТИД «ДС», 2001. – 688 с.
32. Донцов Д. Как защитить компьютер от ошибок, вирусов, хакеров / Д. Донцов. – СПб. : Питер, 2007. – 144 с.
33. Донцов Д. Как сохранить зрение при работе на компьютере / Д. Донцов. – СПб. : Питер, 2007. – 160 с.
34. Дроб’язко В. С. Охорона баз даних: міжнародні, регіональні, національні аспекти : монографія / В. С. Дроб’язко. – К. : ТОВ «Лазурит – Поліграф», 2008. – 132 с.
35. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
36. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
37. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
38. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

39. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика : навчальні посібник / А. В. Дудатьєв, О. П. Войтович, В. А. Каплун. – Вінниця : ВНТУ, 2010. – 219 с.
40. Задірака В. К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : навчальний посібник / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С. Олексюк. – Київ – Тернопіль : Підручники і посібники, 2007. – 272 с.
41. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України. – 1994. – № 31. – С. 286.
42. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).
43. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).
44. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 80/94-ВР (Зі змінами, внесеними згідно із Законом № 1703-IV від 11.05.2004, в редакції Закону № 2594-IV від 31.05.2005, ВВР, 2005, № 26, ст. 347).
45. Закон України «Про інформацію» № 2657-ХИ від 02.10.1992 // ВВР. – 1992. – № 48, ст. 650.
46. Законодавчі та нормативні документи України у сфері інформації, 3-19 видавничої та бібліотечної справи : темат. добірка. У 2 ч. / уклад. Т. Ю. Жигун. – 3-тє вид., допов. – К. : Кн. палата України, 2007. Ч. 1: Правове регулювання у сфері інформації. – 176 с.
47. Захист інформації в комп'ютерних системах та мережах : методична розробка / Б. Я. Корнієнко, Л. М. Щербак. – К. : НАУ, 2006. – 64 с.
48. Захист інформаційних ресурсів України : проблеми і шляхи їх розв'язання / Й. У. Мастяниця, О. В. Соснін, Л. Є. Шиманський ; під редакцією О. В. Сосніна ; Національний інститут стратегічних досліджень. – К., 2000.
49. Захист програмних продуктів : навчальний посібник / В. С. Блінцов, С. С. Козирєв. – Миколаїв : НУК, 2010. – 146 с.
50. Искусство взлома и защиты систем / Дж. Козиол, Д. Личфилд, Д. Эйтэл, К. Энли и др. – СПб. : Питер, 2006. – 416 с.
51. Інформаційні потоки в глобальних комп'ютерних мережах / О. Г. Додонов, Д. В. Ланде, В. Г. Путятін. – К. : Наук. думка, 2009. – 295 с.

52. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Харків : Вид. ХНЕУ, 2009. – 368 с.

53. Кириленко Н. М. Інформаційна безпека : навчально-методичний посібник / Н. М. Кириленко ; Вінницький держ. пед. ун-т ім. М. Коцюбинського. – Вінниця : Глобус-Прес, 2011. – 215 с.

54. Ковальчук В. Н. Система інформаційної безпеки навчального комп'ютерного комплексу : методичний посібник. – Житомир : Вид-во ЖДУ ім. І. Франка, 2009. – 84 с.

55. Кожевніков Г. К. Захист даних в комп'ютерних мережах [Електронний ресурс] : конспект лекцій для студ. спец. 6.010104.06 Професійна освіта. Комп'ютерні технології в управлінні та навчанні. Ч. 2 / Г. К. Кожевніков, Т. С. Бондаренко ; Укр. інж.-пед. акад. – Х. : [б. в.], 2013. – 108 с.

56. Коляда М. Г. Професійна підготовка майбутніх фахівців із захисту інформації та управління інформаційною безпекою: теоретико-методологічний аспект. Монографія / Михайло Георгійович Коляда. – Донецьк : ДВНЗ «ДонНТУ». 2010. – 300 с.

57. Компьютерная преступность : конспект лекций по курсу «Информационная безопасность» / Д. Л. Орловский, О. Ю. Чередниченко. – Харьков : НТУ «ХПИ», 2006. – 64 с.

58. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру. Страсбург, 28 січня 1981 року // www.iu.org.ua

59. Конвенція про захист прав людини і основоположних свобод (Рим, 4.XI.1950) // www.iu.org.ua

60. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; под ред. В. А. Хорошко. – К. : Арий, 2008.

61. Методи та засоби кодування, захисту й ущільнення інформації // Тези доповідей Третьої Міжнародної науково-практичної конференції, м. Вінниця, 20-22 квітня 2011 року. – Вінниця : ВНТУ, 2011. – 231 с.

62. Мухин В. Е. Риск-ориентированная информационная безопасность : монография / В. Е. Мухин ; М-во образования и науки, молодежи и спорта Украины, НТУУ «КПИ». – К., 2011. – 291 с.

63. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанова з керування мережною безпекою. Ст. 1754.

64. НД ТЗІ 1.1-002-99 : Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

65. НД ТЗІ 1.4-001-2000 : Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.

66. НД ТЗІ 2.5-004-99 : Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

67. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

68. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

69. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

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

71. Організаційно-правові основи захисту інформації з обмеженим доступом. Навчальний посібник / за ред. В. С. Сідака. – К., 2006.

72. Основи інформаційної безпеки. Навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. Вінниця : ВНТУ, 2013. – 221 с.

73. Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ... 22.05.98 р. № 505/98 // Уряд. кур'єр. 1998. – 9 липня. – С. 2.

74. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М. : Бином-Пресс, 2002. – 384 с.

75. Селиванов М. В. Защита прав на компьютерную программу: теория и практика. Учебно-практическое пособие / М. В. Селиванов. – Харьков : Эспада, 2004. – 176 с.

76. Терейковський І. А. Нейронні мережі в засобах захисту комп'ютерної інформації / І. А. Терейковський. – К. : ТОВ «ПоліграфКонсалтинг», 2007. – 209 с.

77. ТЗІ 1.1-003-99 : Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

78. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

79. Филиппова Л. Я., Зеленецкий В. С. Компьютерная этика. Морально-этические и правовые нормы для пользователей компьютерных сетей : учеб. пособие / Л. Я. Филиппова, В. С. Зеленецкий. – Харьков : Изд-во «Кроссроуд», 2006. – 212 с.

80. Хараберюш І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія / І. Ф. Хараберюш, В. Я. Мацюк, В. А. Некрасов, О. І. Хараберюш. – К : КНТ, 2007. – 196 с. (Серія: Проблеми оперативно-розшукової діяльності).

81. Шорошев В. В. Основи формування політики безпеки комп'ютерних систем : монографія / В. В. Шорошев. – К. : ДУІКТ, 2011. – 257 с.

82. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем : монографія / В. В. Шорошев. – К. : ДУПСТ, 2011. – 257 с.

Навчальний посібник

С. М. Яшанов, М. С. Яшанов

БЕЗПЕКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Технічний редактор – О. Гордашевська
Макетування – Т. Меркулова

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО ПЕДАГОГІЧНОГО УНІВЕРСИТЕТУ
ІМЕНІ М. П. ДРАГОМАНОВА

Підписано до друку *12 квітня* 2018 р.
Формат 60x84/16. Папір офісний. Гарнітура Times New Roman.
Ум. др. арк. 15,93. Об.-вид. арк. 9,78.
Наклад 300 прим. Зам №
Віддруковано з оригіналів

Видавництво Національного педагогічного університету
імені М. П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9.
Свідоцтво про реєстрацію ДК № 1101 від 29.10.2002 (044) 234-75-87
Віддруковано в друкарні Національного педагогічного університету
імені М. П. Драгоманова (044) 239-30-26