Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

на тему: **" Базові системи захисту"**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки)

ПЛАН ЛЕКЦІЇ

1. Рівні інформаційно-комунікаційної системи.
2. Функціональні сервіси безпеки та їх механізми.
3. Основні підсистеми комплексу засобів захисту.

ЛІТЕРАТУРА

1. **Андрианов В.И., Бородин В.А., Соколов А.В.** "Шпионские штучки" и устройства для защиты объектов и информации: Справочное пособие. – СПб.: Лань, 1996. – 272 с.
2. **Прохоров И.В., Толстой А.И.** Телекоммуникационные сети: Учебное пособие. – М.: МИФИ, 1996. – 64 с.
3. **Зегжда Д.П., Ивашко А.М.** Как построить защищенную информационную систему. Том 1. - СПб: НПО «Мир и семья - 95», 1997. - 312 с.

1. Рівні інформаційно-комунікаційної системи.

Інформаційно-комунікаційні системи на перший погляд абсолютно різні. Проте, порівнюючи їх, можна відзначити певні спільні риси. Для організації конкретного профілю (наприклад, профілю страхової компанії, виробничого об'єднання, органу державної влади тощо) є своя інформаційно-комунікаційна система. Кожна з ІКС має типові рівні, на яких вирішуються спільні для всіх систем задачі. Зазвичай розглядають чотири рівні (рис. 1)

Рис. 1. Рівні інформаційно-комунікаційної системи

1. Рівень мережі - відповідає за взаємодію вузлів ІКС.

Елементами ІКС, що належать до цього рівня, є модулі, які реалізують стеки протоколів мережної взаємодії, наприклад TCP /IP. Також на цьому рівні функціонує специфічна апаратура - мережне обладнання.

2. Рівень операційних систем - відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням. Серед типових представників цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris і Linux.

3. Рівень систем керування базами даних (СКБД) - відповідає за зберігання та оброблення даних. Серед типових представників цього рівня можна назвати СКБД Oracle, а також MS SQL Server. Іноді СКБД є центральним елементом ІКС (наприклад, облік товарів на складі), а іноді виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІКС.

4. Рівень прикладного ПЗ - включає прикладний компонент і компонент подання. Прикладний компонент забезпечує виконання специфічних функцій ІКС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. У різних варіантах архітектури ІКС прикладний компонент і компонент подання можуть міститися на одному або на різних комп'ютерах (компонент подання - на робочій станції клієнта, прикладний компонент – на сервері застосувань). На рівні прикладного ПЗ функціонують офісні застосування (наприклад, Microsoft Office, Star Office або Open Office), бухгалтерські програми, спеціально розроблені для кожної окремої ІКС програмні засоби, що реалізують специфічні для системи функції, та будь-які інші програми.

Порушники можуть впливати на ІКС на будь-якому з цих рівнів. Кожному з них притаманні характерні вразливості, а відтак - різні засоби захисту. Приклад типової інформаційно-комунікаційної системи зображено на Рис. 2

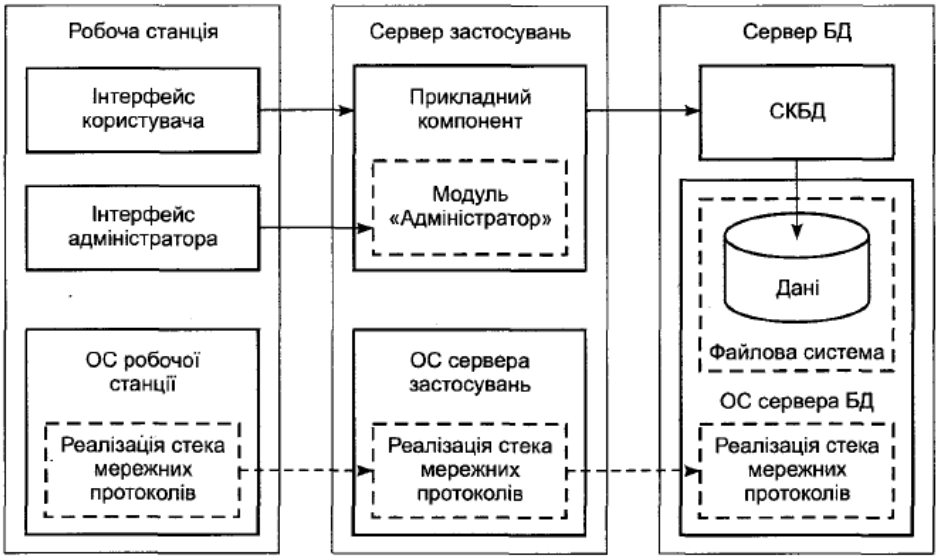


Рис. 2. Структура інформаційно-комунікаційної системи

База даних системи містить конфіденційні дані, які становлять інтерес для порушника. З об'єктами, що містять дані, пов'язані службові об'єкти, які містять атрибути доступу, що визначають, які користувачі або групи користувачів мають право читати або модифікувати об'єкт. Легальні користувачі цієї системи використовують прикладний інтерфейс, який здійснює доступ до бази даних за допомогою визначених процедур, що транслюють дії користувача у специфічні SQL запити, які, зокрема, перевіряють права доступу. За звичайних дій користувача гарантується коректність запитів. Для доступу до інтерфейсу користувач має ввести ідентифікатор і пароль. Повноваження користувача визначаються його належністю до наперед заданих груп; керування повноваженнями користувачів і атрибутами доступу об'єктів здійснює спеціально вповноважений користувач – так званий адміністратор безпеки. Він має свій інтерфейс керування, доступ до якого також захищений паролем.

Порушник має можливість здійснити доступ до захищених даних на рівні прикладного ПЗ (рис. 3). Для цього він може спробувати добрати пароль іншого користувача, якому доступ до цієї інформації дозволено, або отримати доступ із правами адміністратора і змінити права доступу до захищених об'єктів чи власні повноваження. Зрештою, він може спробувати знайти вразливість у прикладній програмі або скористатися відомою вразливістю. З цією метою порушнику доведеться створити певний специфічний запит, не передбачений розробниками програмного забезпечення (у найпростішому випадку додати до текстового рядка спеціальні керуючі символи або ввести числові значення, що виходять за межі дозволеного діапазону), у відповідь на який система надасть йому несанкціонований доступ.

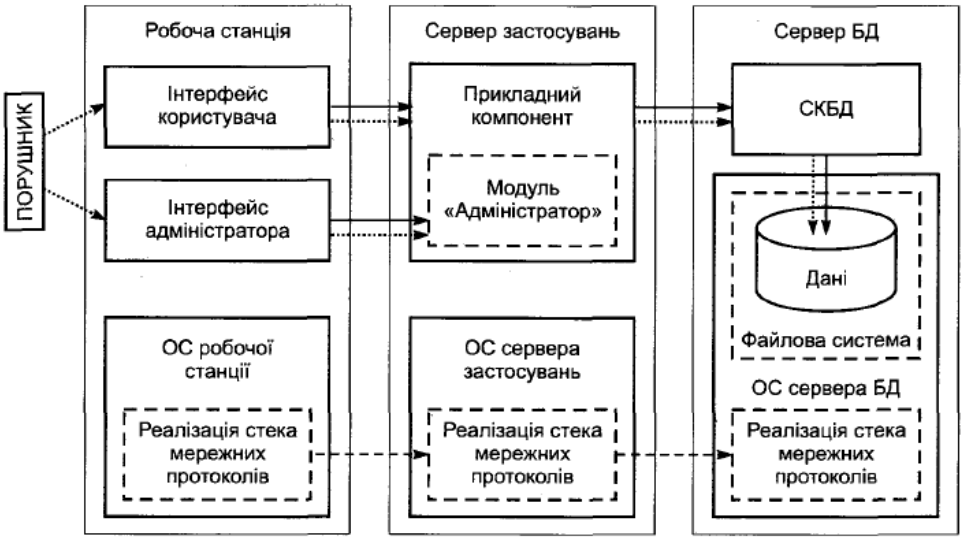


Рис. 3. Несанкціонований доступ на рівні прикладного ПЗ

Інший шлях - доступ на рівні СКБД. Такий доступ порушник здійснює в обхід прикладного ПЗ безпосередньо до бази даних (рис. 4). Для цього він може згенерувати специфічний SQL-запит або скористатися засобами самої СКБД для перегляду таблиць даних.

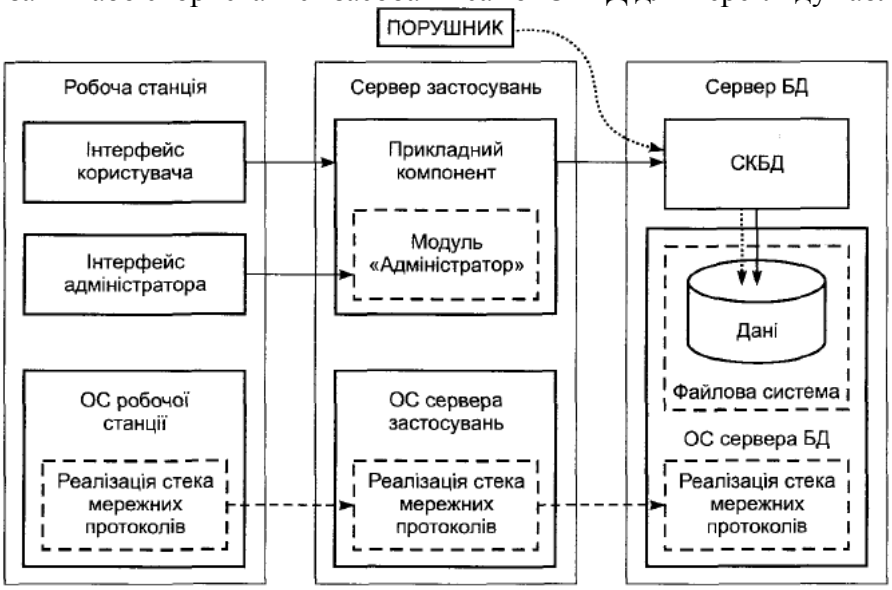


Рис. 4. Несанкціонований доступ на рівні СКБД

Нарешті, порушник може спробувати здійснити доступ на рівні ОС. Зокрема, такий доступ може полягати у несанкціонованому копіюванні файлів бази даних засобами файлової системи сервера (рис. 5).

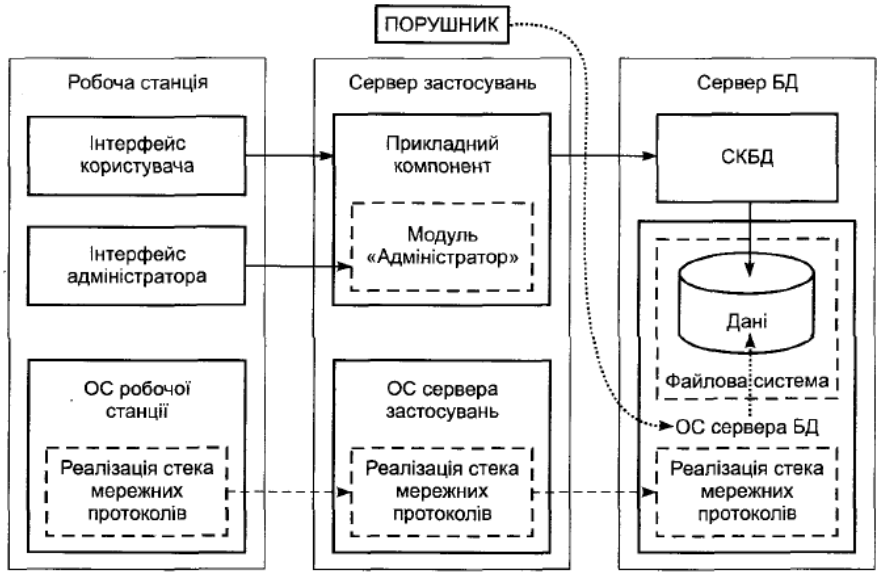


Рис. 5. Несанкціонований доступ на рівні ОС

Розглянуті рівні доступу передбачають наявність у користувача деяких повноважень у системі та доступу до її інтерфейсів. Останній рівень доступу - рівень мережі - потенційно може надати доступ користувачу, який не лише не має повноважень у системі, а й знаходиться поза її межами. На цьому рівні можлива атака на дані, які передаються у мережі, а. також вплив через мережні засоби на вузли системи - сервери і робочі станції, внаслідок чого може бути створено передумови для доступу на вищих рівнях, наприклад, створено обліковий запис користувача- порушника з правами адміністратора (рис. 6).

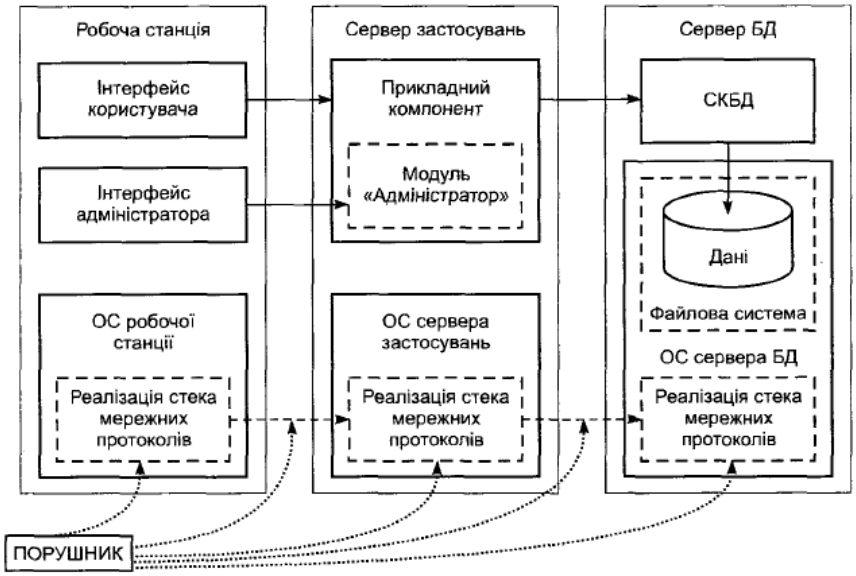


Рис. 6. Несанкціонований доступ на рівні мережі

2. Функціональні сервіси безпеки та їх механізми.

Засоби захисту системи забезпечують кілька функціональних сервісів. ***Функціональний сервіс*** - це визначений набір функцій, які дають змогу протистояти певній множині загроз (у вітчизняних нормативних документах застосовано термін «функціональна послуга безпеки»). Для їх реалізації задіюють специфічні механізми. У табл. 1 наведено основні узагальнені сервіси безпеки для мережного рівня ІКС і механізми, що їх реалізують.

Таблиця 1. Класифікація основних функціональних сервісів і механізмів, що їх реалізують

Сервіси	**Механізми**	**Забезпечують**		
Керування доступом	**Керування доступом**	**конфіденційність**	**цілісність**	**доступність**
Конфіденційність	Шифрування	+		
	Заповнення трафіку	+		
	Керування маршрутом	+		
Цілісність	Шифрування		+	
	Керування доступом		+	
	Код справжності повідомлення		+	
	Повтор повідомлень		+	
	Електронний цифровий підпис		+	
Доступність	Керування маршрутом			+
	Керування доступом			+
Причетність до отримання	Електронний цифровий підпис		+	
	Завірення		+	

Таксономія функцій систем захисту

Сервіси безпеки, як правило, здатні забезпечувати захист інформаційно-комунікаційних систем від виникнення загроз як навмисно спричинених, так і випадкових.

Розглядають такі рівні захисту.

1. Рівень захисту від несанкціонованого доступу до ресурсів системи.

На цьому рівні реалізовано такі механізми:

- ідентифікація;

- автентифікація;
- керування доступом;
- шифрування;
- контроль справжності інформації;
- знищення залишкових даних;
- захист від комп'ютерних вірусів.

2. Рівень захисту від несанкціонованого використання ресурсів системи.
На цьому рівні реалізовано:

- контроль за виділенням ресурсів, квоти;
- контроль за складом програмних засобів ІКС;
- захист програм від копіювання, дослідження, модифікації та несанкціонованого запуску.

3. Рівень захисту від некоректного використання ресурсів системи.
На цьому рівні реалізовано такі механізми:

- ізолювання ділянок оперативної пам'яті;
- підтримка цілісності та несуперечності даних;
- попередження користувача перед виконанням небезпечних дій.

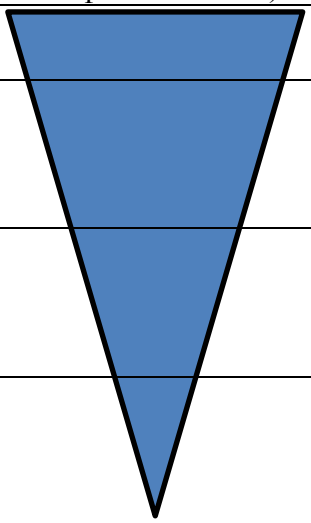
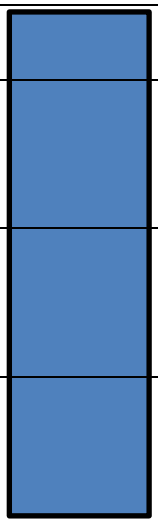
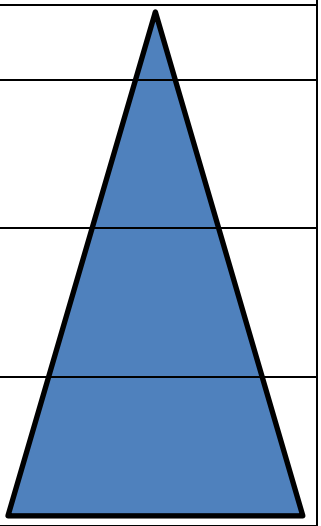
4. Рівень внесення інформаційної та функціональної надмірності.
На цьому рівні здійснюються:

- резервування інформації;
- тестування і самотестування;
- відновлення і самовідновлення;
- дублювання компонентів.

Сервіси рівнів 1 і 2 захищають від несанкціонованих дій користувачів і програмних засобів, тобто здебільшого від реалізації навмисних загроз. Рівні 3 та 4 захищають від реалізації загроз, які були ненавмисно спричинені персоналом або виникли випадково.

Слід зазначити, що сервіси всіх рівнів роблять свій внесок у захист конфіденційності, цілісності та доступності інформації. У табл. 2 показано, як співвідносяться внески різних рівнів захисту в забезпечення певних властивостей інформації.

Таблиця 2. Захист на різних рівнях ІКС

Рівні захисту / Цілі захисту	Захист від викрадання інформації (загрози конфіденційності)	Захист від втрати та підробки інформації (загрози цілісності)	Захист від збоїв і відмов (загрози доступності)
Захист від НСД до ресурсів системи			
Захист від несанкціонованого Використання ресурсів системи			
Захист від некоректного використання ресурсів системи			
Рівень внесення інформаційної й функціональної надлишковості			

Зверніть увагу на те, що розглянуті в таблиці рівні захисту і рівні ІКС є взаємно ортогональними. Елементи (тобто окремі механізми) кожного рівня захисту можуть бути реалізовані на всіх рівнях ІКС. Приклади таких реалізацій зведено у табл. 3.

Таблиця 3. Механізми захисту на різних рівнях ІКС

Рівні захисту	Рівні інформаційної системи			
	Мережні сервіси	**ОС**	**СКБД**	**Застосування**
Захист він НСД до ресурсів системи	Ідентифікація мережних пристроїв за IP та MAC-адресами. Ідентифікація співтовариства SNMP. Автентифікація користувачів (протоколи EAPOL, RADIUS). Сегментація мережі. Віртуальні локальні мережі (VLAN). Міжмережне екранування (брандмауери). Керування маршрутом пакетів. Шифрування трафіку. Віртуальні приватні мережі (VPN)	Ідентифікація й автентифікація користувачів. Автентифікація об'єктів доступу. Керування доступом користувачів до об'єктів. Шифрування даних автентифікація. Шифрування журналів реєстрації. Очищення ділянок оперативної пам'яті, що звільняються. Очищення дискового простору, що звільняється	Ідентифікація й автентифікація користувачів. Керування доступом до таблиць, записів, процедур. Знищення залишкових даних	Ідентифікація й автентифікація користувачів. Керування доступом до інтерфейсів, програмних модулів, даних. Шифрування даних. Накладання і перевірка електронного цифрового підпису. Захист від комп'ютерних вірусів — антивірусне ПЗ
Захист від несанкціонованого використання ресурсів системи	Контроль за виділенням ресурсів окремим інформаційним потокам. Якість обслуговування (QoS). Контроль за складом апаратних і програмних	Планування процесорного часу. Контролі» за виділенням оперативної пам'яті. Квоти на використання дискового простору. Контроль	Контроль за виділенням ресурсів С К БД, квоти. Контроль за складом збережених процедур. Контроль доступу до використання збережених	Контроль за виділенням ресурсів. Контроль за складом програмних засобів ІКС. Захист програм від копіювання, дослідження, модифікації.

	засобів мережі. Апаратна реалізація функцій, захист віл дослідження і модифікації	цілісності компонентів ОС. Захист від налагодження програм	процедур	Контроль доступу до запуску програм та (або) окремих процедур на виконання
Захист від некоректного використання ресурсів системи	Сегментація мережі. Контроль цілісності пакетів (CRC). Контроль послідовності пакетів. Протокол STP. Віртуальні локальні мережі (VLAN')	Ізолювання ділянок оперативної пам'яті. Підтримка цілісності та несуперечності технологічної інформації (файлова система, системний реєстр тощо). Попередження користувача перед виконанням небезпечних дій	Підтримка цілісності та несуперечності даних. Попередження Користувача перед виконанням небезпечних дій	Підтримка власного домену виконання. Контроль цілісності, несуперечності та коректності даних. Попередження користувача перед виконанням небезпечних дій
Рівень внесення інформаційної й функціональної надлишковості	Тестування і самотестування обладнання. Відновлення і самовідновлення обладнання. Відновлення і самовідновлення ТТЗ (завантаження із централізованого сервера). Централізоване резервування і відновлення (самовідновлення) конфігураційної інформації. Резервування каналів зв'язку (STP, VRRP).	Резервування інформації на рівні файлової системи і обладнання (RAID). Тестування і самотестування обладнання та системних програмних засобів. Відновлення і самовідновлення операційного середовища. Дублювання окремих пристроїв. Дублювання серверів	Резервування інформації на рівні СКБД. Дзеркал ювання. Створення резервних копій. Тестування і самотестування цілісності даних. Відновлення та самовідновлення даних із резервних копій. Розподілені БД	Резервування інформації на прикладному рівні. Тестування і самотестування програмного забезпечення. Відновлення і самовідновлення програмного забезпечення. Дублювання програмних компонентів

	Агрегація каналів, балансування навантаження			

3. Основні підсистеми комплексу засобів захисту.

Комплекс засобів захисту - це сукупність підсистем, які забезпечують необхідні сервіси безпеки. На рис. 7 показано типову структуру КЗЗ.

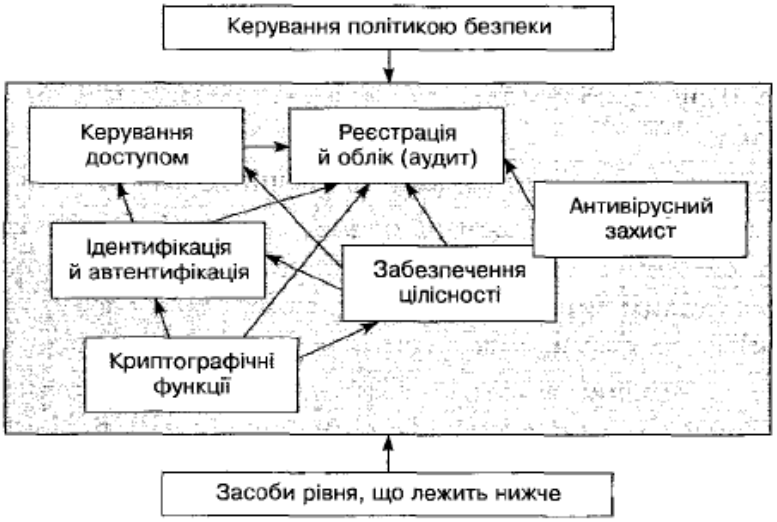


Рис. 7. Структура КЗЗ і взаємозв'язки підсистем

Така структура може бути реалізована повністю або (частіше) частково на всіх рівнях ІКС. Розглянемо призначення, будову і взаємодію основних підсистем.

Підсистема керування доступом

Підсистема керування доступом є центральною підсистемою захисту від НСД. Завдання підсистеми керування доступом полягає у реалізації політики безпеки як певного набору правил розмежування доступу.

Здійснення доступу може змінювати стан системи (наприклад, після запуску програми на виконання утворюється новий процес) та (або) утворювати інформаційні потоки від одного об'єкта до іншого (наприклад, читання або записування інформації). Таким чином, ознаками доступу є не лише суб'єкт і об'єкт, а й метод доступу (рис. 8).

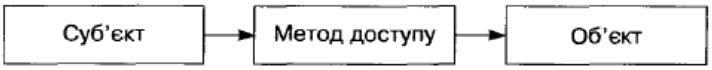


Рис. 8. Схема здійснення доступу

Можна навести чимало прикладів методів здійснення доступу, які залежать ще й від типу об'єкта. Перелічимо деякі з них:

- читання;
- записування (під записуванням розуміють будь-яке модифікування вмісту об'єкта, включаючи повну заміну або видалення вмісту);
- додавання (записування в об'єкт додаткової інформації без можливості змінювання тих даних, які вже містяться в об'єкті);
- виконання (для файлового об'єкта це досить складна послідовність дій, яка приводить до виконання процесором інструкцій, що містяться в об'єкті);
- читання атрибутів захисту;
- записування атрибутів захисту;
- зміна власника;
- видалення об'єкта (не слід плутати з видаленням вмісту об'єкта).

Підсистема керування доступом на основі атрибутів, асоційованих із суб'єктами і об'єктами системи, дозволяє або забороняє окремі акти доступу за визначеними методами і

таким чином забезпечує розмежування доступу користувачів і процесів (суб'єктів) до захищених об'єктів згідно зі встановленими правилами. Правила встановлюють відповідно до обраної політики керування доступом, яка може бути описаною у термінах моделі відповідної політики. Найпоширенішими є дві моделі керування доступом - **дискреційна** і **мандатна.**

Дискреційне керування доступом (Discretionary Access Control) дає змогу довільним чином обмежувати права доступу до кожного окремого об'єкта системи за наявності власника в кожного з них. Правила розмежування доступу в разі дискреційного керування можна описати за допомогою **матриці доступу**. На практиці ж найчастіше використовують **списки доступу** (Access Control Lists, ACL), які асоціюються з кожним захищеним об'єктом у системі та містять ідентифікатори різних суб'єктів разом з їхніми правами доступу до цього об'єкта.

Політика безпеки інформації містить не лише опис ПР Д, але й обмеження, що накладаються на спосіб модифікації цих правил (наприклад, списків доступу). Якщо застосовують довірче керування доступом, усі права на змінення прав доступу до об'єкта надаються (довіряються) суб'єкту, який є власником цього об'єкта, а якщо адміністративне - система захисту визначає можливість доступу суб'єктів до об'єктів на основі атрибутів доступу, які може встановлювати або змінювати лише спеціально призначений адміністратор.

Мандатне керування доступом (Mandatory Access Control), яке ще називають нормативним або примусовим, можна реалізувати у разі адміністративного керування. Суть мандатного керування доступом полягає у тому, що з кожним об'єктом, пасивним і активним (суб'єктом), асоціюють так звану мітку безпеки, яка визначає рівень цього об'єкта у деякій ієрархії рівнів. Можливість доступу визначають порівнянням міток безпеки суб'єкта й об'єкта на основі певної моделі.

Підсистема ідентифікації й автентифікації

Для того щоб підсистема керування доступом могла виконувати свої функції, вона має бути спроможною розрізняти суб'єкти й об'єкти на основі даних, отриманих від підсистеми ідентифікації й автентифікації. Жоден із суб'єктів не зможе отримати доступ до об'єктів, якщо не надасть системі захисту достатній обсяг інформації про себе. Завдання підсистеми ідентифікації й автентифікації полягає у тому, щоб запитати в суб'єкта таку інформацію, прийняти та перевірити її на відповідність даним, які зберігаються у системі, захистити цю інформацію під час її введення, перевірки та зберігання від несанкціонованого доступу інших суб'єктів, а також видати дані, необхідні для авторизації суб'єкта, тобто для надання йому повноважень у системі. Крім ідентифікації й автентифікації суб'єктів, у разі потреби забезпечується автентифікація об'єктів.

Часто цю підсистему не розглядають окремо, а відносять її функції до підсистеми керування доступом, хоча, на наш погляд, це не зовсім правильно, оскільки результати ідентифікації й автентифікації використовують також інші підсистеми, зокрема підсистема реєстрації.

Нагадаємо, що ідентифікація суб'єкта - це повідомлення системі захисту його унікального ідентифікатора в обчислювальній системі, автентифікація суб'єкта - надання системі захисту крім ідентифікуючої інформації відомостей, за допомогою яких система перевіряє його дійсність, авторизація суб'єкта - це процедура надання йому визначених у системі повноважень, яка відбувається після вдалих ідентифікації та автентифікації.

Відтак, щоб отримати доступ до обчислювальної системи, користувачу потрібно спочатку ідентифікувати себе, а механізми захисту мають підтвердити його ідентифікатор. Якщо перевіряється істинність лише користувача, то таку процедуру називають одностороннім (Peer Entity) підтвердженням істинності. Коли користувач має підтвердити свою істинність системі, а система, у свою чергу, - свою істинність користувачу, таку процедуру називають двосторонньою (Peer to Peer) автентифікацією.

Є три способи підтвердження істинності користувача, відповідно до яких механізми підсистеми ідентифікації та автентифікації мають перевірити:

- інформацію, відому лише користувачу та системі автентифікації (паролі, ідентифікаційні коди тощо);
- додаткові відомості, для таємного зберігання яких застосовують знімні пристрої (ключі, магнітні чи смарт-картки);

- дані, які є індивідуальними характеристиками кожної особи (відбитки пальців, малюнок сітківки ока, голосові характеристики, особливості користування клавіатурою та маніпуляторами).

Найбільш поширений - перший спосіб.

Підсистема забезпечення цілісності

Підсистема забезпечення цілісності здійснює контроль цілісності всіх інформаційних ресурсів. Контроль, як правило, здійснюється під час запуску системи чи програм на виконання (коли утворюються нові процеси). Для особливо критичних інформаційних і програмних ресурсів (наприклад, апаратних і програмних компонентів КЗЗ, системного програмного забезпечення, баз даних, об'єктів, що містять інформацію з обмеженим доступом) контроль може здійснюватися неперервно. Також ця підсистема попереджає про порушення цілісності та надає засоби для відновлення системи захисту від НСД.

Типовим механізмом реалізації контролю цілісності є підраховування контрольних сум файлів перед запуском останніх на виконання та порівняння цих значень з еталонними сумами. Для обчислення контрольних сум часто використовують швидкі алгоритми (наприклад, CRC32), які достатньо надійно діють у разі перевірки відсутності випадкових порушень цілісності файлу (наприклад, відсутності помилок під час пересилання файлу через телекомунікаційну мережу), але не можуть унеможливити підробку контрольної суми, коли порушник навмисно модифікує файл. Значно надійнішим, хоча й повільнішим, є обчислення хеш-функції, яке застосовують у спеціалізованих системах контролю цілісності, призначених для захисту від дій зловмисників.

Криптографічна підсистема

Криптографічна підсистема забезпечує такі механізми захисту:

- шифрування та дешифрування даних;
- хешування;
- накладання електронного цифрового підпису;
- генерування ключів.