Глава 1.
Предмет захисту

1.1. Властивості, види і форми представлення інформації

Інформація - ***це результат відображення і обробки в людській свідомості різноманітності довкілля, це відомості про предмети і явища природи, що оточують людину, повідомлення про діяльність інших людей і т.п***. Відомості, якими людина з допомогою машини обмінюється з іншою людиною або з машиною, і є предметом захисту. Однак захисту підлягає не будь-яка інформація, а тільки та, що має цінність. Цінною стає та інформація, володіння якою дозволить її теперішньому чи потенційному власнику отримати який-небудь виграш: моральний, матеріальний, політичний і т.д. Оскільки в людському суспільстві завжди існують люди, що бажають незаконним шляхом отримати цінну інформацію, у її власника виникає необхідність в її захисті.

Цінність інформації є критерієм при прийнятті будь-якого рішення про її захист. Хоча було зроблено багато різних спроб формалізувати цей процес з використанням методів теорії інформації і аналізу рішень, процес оцінки до сих пір залишається досить суб’єктивним.

Глава 1.
Предмет захисту

Відомий такий розподіл інформації за рівнем важливості.

1) ***життєво важлива*** - незамінима інформація, наявність якої необхідна для функціонування організації;
2) ***важлива інформація*** - інформація, що може бути замінена чи відновлена, але процес відновлення дуже складний і пов’язаний з великими затратами;
3) ***корисна інформація*** - інформація, яку важко відновити, але організація може ефективно працювати і без неї
4) ***неістотна інформація*** - інформація, яка більш не потрібна організації.

На практиці віднесення інформації до однієї з цих категорій може бути дуже складною задачею, оскільки та сама інформація може бути використана багатьма підрозділами організації, кожен з яких може віднести цю інформацію до різних категорій за рівнем важливості. ***Категорії важливості, як і цінність інформації, звичайно змінюються з часом і залежать від ступені відношення до неї різних груп споживачів і потенційних порушників***.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Існують визначення груп осіб, пов’язаних з обробкою інформації: ***тримач*** - організація чи особа - власник інформації; ***джерело*** - організація чи особа, що постачає інформацію; ***порушник*** - окрема особа чи організація, що прагне отримати інформацію.

Відношення цих груп до значимості однієї і тієї ж інформації може бути різним: для однієї - важлива, для другої – ні. Наприклад: важлива оперативна інформація, така, наприклад, як список замовлень на даний тиждень і графік виробництва, може мати високу цінність для тримача, тоді як для джерела (наприклад, замовника) чи порушника низька; персональна інформація, наприклад медична, має значно більшу цінність для джерела (особи, до якої відноситься інформація), чим для її тримача чи порушника; інформація, що використовується керівництвом для формування рішень, наприклад про перспективи розвитку ринку, може бути значно більш цінною для порушника, ніж для джерела чи її тримача, який вже завершив аналіз цих даних. Наведені категорії важливості можуть бути використані для будь-якої інформації.

Глава 1.
Предмет захисту

Це також узгоджується з існуючим принципом поділу інформації за рівнем секретності. Рівень секретності - це адміністративна чи законодавча міра, що відповідає мірі відповідальності особи за витік чи втрату конкретної секретної інформації, яка регламентується спеціальним документом, з врахуванням державних, військово-стратегічних, комерційних, службових чи приватних інтересів. Такою інформацією може бути державна, військова, комерційна, службова чи особиста таємниця. Наприклад: важлива оперативна інформація, така, наприклад, як список замовлень на даний тиждень і графік виробництва, може мати високу цінність для тримача, тоді як для джерела (наприклад, замовника) чи порушника низька; персональна інформація, наприклад медична, має значно більшу цінність для джерела (особи, до якої відноситься інформація), чим для її тримача чи порушника; інформація, що використовується керівництвом для формування рішень, наприклад про перспективи розвитку ринку, може бути значно більш цінною для порушника, ніж для джерела чи її тримача, який вже завершив аналіз цих даних.

Глава 1.

Предмет захисту

Наведені категорії важливості можуть бути використані для будь-якої інформації. ***Практика довела, що захищати потрібно не тільки секретну інформацію. Несекретна інформація, що зазнала несанкціонованих змін (наприклад, модифікації команд управління), може призвести до витоку чи втрати пов’язаною з нею секретної інформації, а також до невиконання автоматизованою системою заданих функцій, що спричинено отриманням хибних даних, які можуть бути не виявлені користувачем системи***.

Лекція 1

Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Сумарна кількість, чи статистика несекретних даних, в результаті може бути секретною. Аналогічно збірні дані одного рівня секретності в цілому можуть бути інформацією більш високого рівня секретності. Для захисту від подібних ситуацій широко використовується розмежування доступу до інформації за функціональною ознакою. ***При однаковому ступені важливості інформації, що опрацьовується в системі обробки даних, інформація ділиться у відповідності з функціональними обов’язками і повноваженнями користувачів, які встановлюються адміністрацією організації - власника АСОД.*** У відповідності до описаних принципів поділу інформацію за категоріями важливості і секретності зобразити у вигляді піраміди, що складається з декількох шарів по вертикалі. ***Вершиною піраміди*** є найбільш важлива інформація, а ***фундаментом*** - несекретна інформація, пов’язана з обробкою більш важливої (секретної) інформації. ***Кожний шар даної піраміди, поділений на частини по горизонталі, віддзеркалює принцип поділу інформації за функціональною ознакою і повноваження її користувача*** (рис.1.1)

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

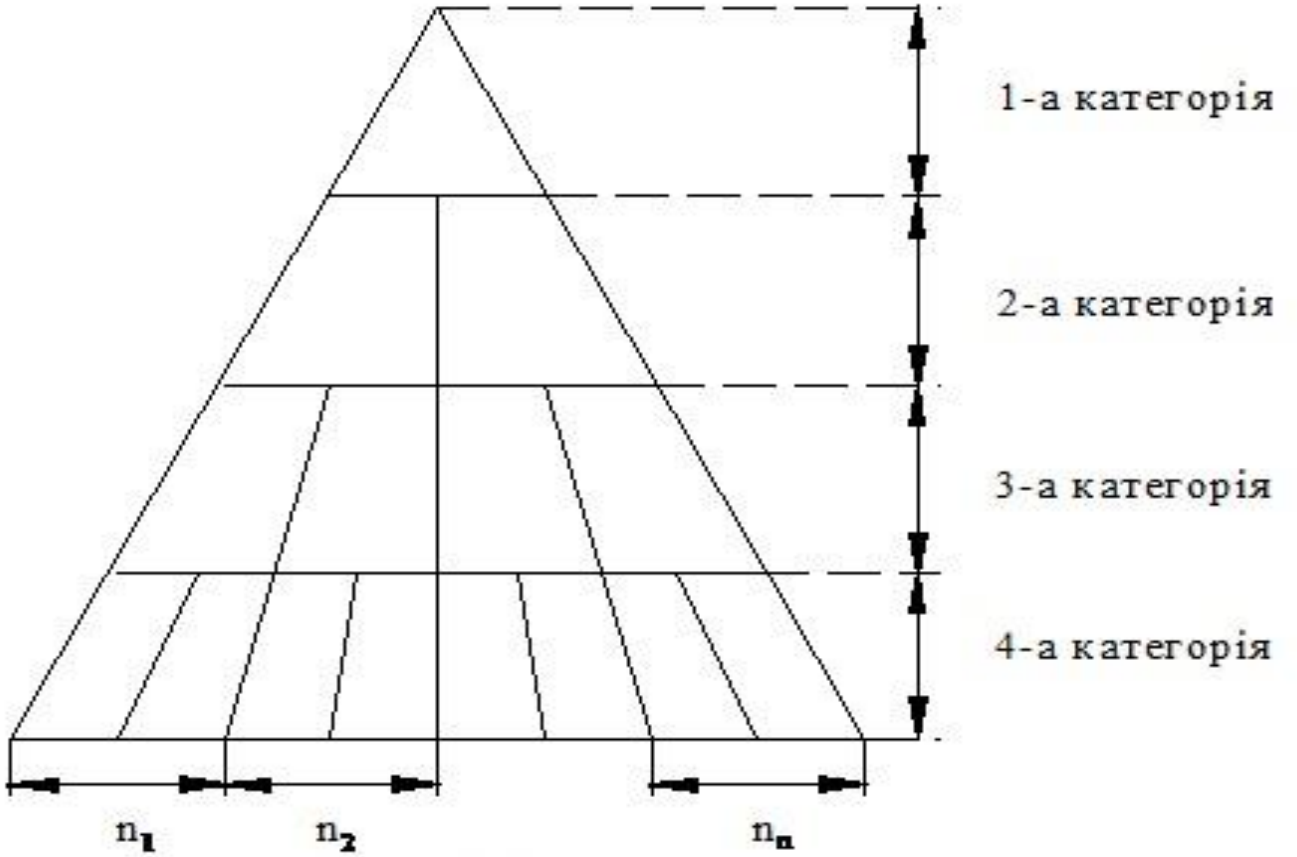


Рис. 1.1. Модель предмету захисту

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Безпека інформації в АСОД інтерпретується як: 1) ***небезпека її несанкціонованого отримання*** під час усього часу її знаходження в АСОД; 2) ***безпека дій, для здійснення яких використовується інформація***. Принципові відмінності розширеного трактування у порівнянні з традиційним дуже важливі, так як обчислювальна техніка все більш використовується для автоматизованого і автоматичного управління високовідповідальними інформаційними системами і процесами, в яких несанкціоновані зміни запланованих алгоритмів і технологій можуть мати серйозні наслідки. ***У інформації, що обробляється АСОД є свій життєвий цикл***, який схематично зображений на рис.1.2

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

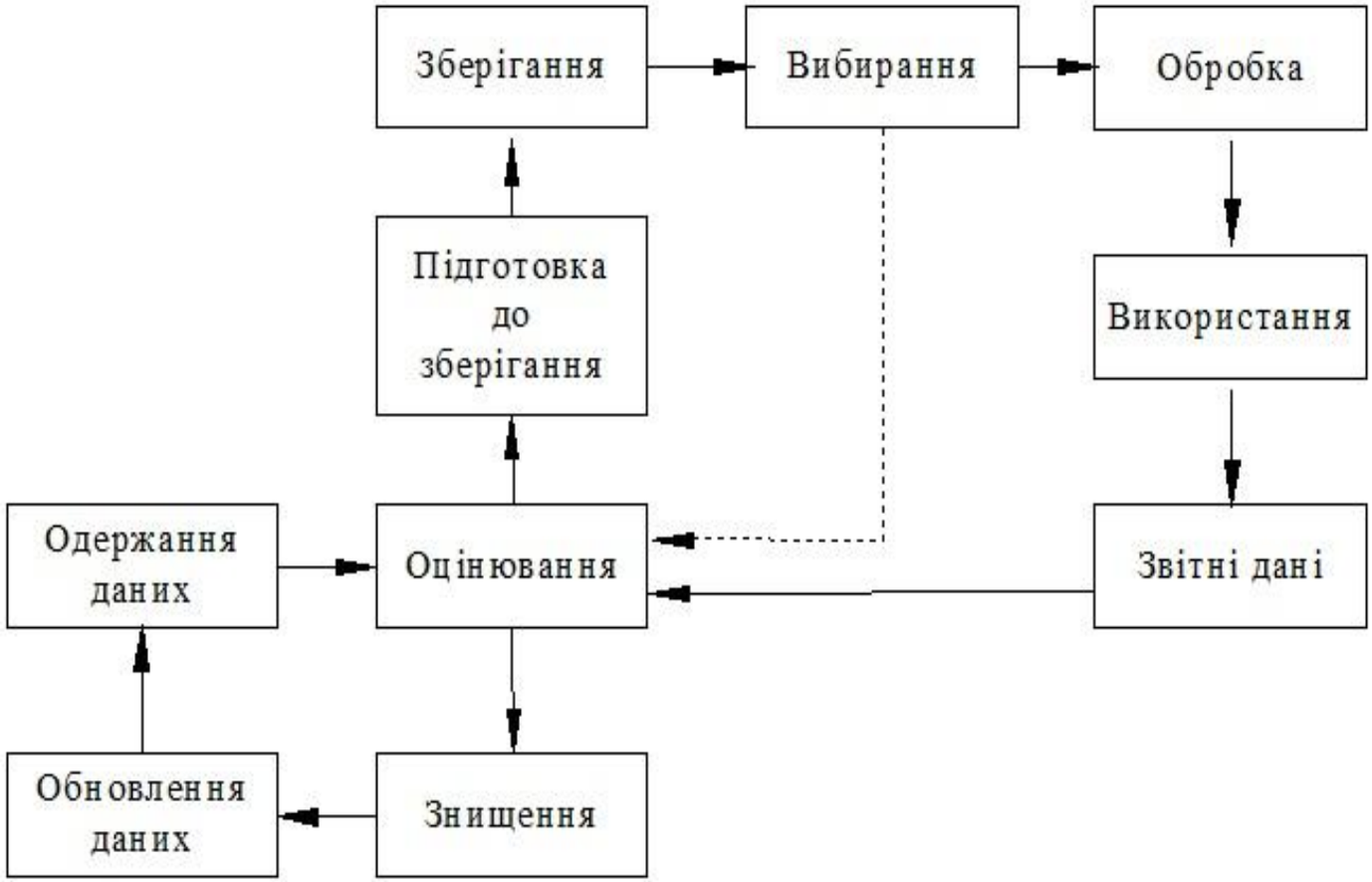


Рис. 1.2. Життєвий цикл інформації

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.

Предмет захисту

Отримана системою інформація оцінюється на достовірність і корисність. Частина інформації знищується, а решта підготовлюється до зберігання (систематизується, перетворюється у зручну для зберігання форму, сортується по масивам зберігання). Із сховища вибирається потрібна в даний момент часу інформація, опрацьовується і використовується з певною метою.

Отримані звітні дані проходять той самий цикл. При вибиранні можуть знищуватись відомості, що втратили інтерес через їх старіння. Кількісні оцінки старіння інформації, що наводяться в літературі досить суперечливі. Час життя інформації визначається її власником в процесі експлуатації АСОД в конкретних умовах.

Інформація, втілена і зафіксована в деякій матеріальній формі, називається повідомленням. Повідомлення можуть бути неперервними і дискретними (цифровими). Неперервне повідомлення є деякою фізичною величиною (електричною напругою, струмом і т.п.), зміна якої віддзеркалює протікання процесу, що розглядається.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.

Предмет захисту

Фізична величина, що передає неперервне повідомлення, може приймати будь-які значення в довільні моменти часу. В неперервному повідомленні скінченої довжини може міститись велика кількість інформації. Для дискретних повідомлень характерна наявність фіксованого набору окремих елементів, з яких дискретні моменти часу формуються різні послідовності елементів. Важливою є не фізична природа елементів, а та обставина, що набір елементів скінчений і тому будь-яке дискретне повідомлення скінченої довжини передає скінчене число значень деякої величини, і отже, кількість інформації в такому повідомленні є скінченою

При дискретній формі представлення інформації окремим її елементам можуть бути присвоєні числові (цифрові) значення. В таких випадках говорять про цифрову інформацію, а обчислювальні машини і системи, що використовують цифрову форму представлення інформації, називають також цифровими. ***Елементи, з яких складаються дискретні повідомлення, називають буквами чи символами. Набір цих букв (символів) утворює алфавіт***.

Лекція 1

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Під буквами розуміються будь-які знаки (звичайні букви, цифри, знаки розділення, математичні і інші знаки і т.п.). Число символів в алфавіті називають об’ємом алфавіту. Об’єм алфавіту визначає кількість інформації , що доставляється одним символом повідомлення. Якщо алфавіт має об’єм A і у будь-якому місті повідомлення імовірність появи будь-якого символу є однаковою, то **кількість інформації**, що передається символом, можна визначити так: $I_0 = \log_2 A\,[\text{біт}]$ (1.1)

Дискретне повідомлення можна розкласти на групи символів і назвати ці групи словами. Довжина слова визначається кількістю символів, що міститься в ньому. В обчислювальній техніці широко використовується однорідне представлення інформації, при якому в обчислювальній системі чи окремих її частинах всі слова мають певну довжину. Однорідне представлення інформації спрощує обмін нею і конструкцію пристроїв обчислювальної системи.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.

Предмет захисту

В алфавіті об’ємом A можна представити N різних слів довжиною S, де:

$$N = A^{s} \quad (1.2)$$

Тоді **кількість інформації**, що міститься в слові, дорівнює:

$$I_1 = \log_2 N = S \log_2 A = S * I_0 \quad (1.3)$$

Вираз (1.3) справедливий, якщо імовірність появи у повідомленні будь-якого слова (і символу) рівні і не залежать від слів (і символів), що їм передують.

Зв’язок між символами повідомлення створює надлишковість інформації. В мові надлишковість носить природній характер. Однак в обчислювальних системах широко використовується штучна надлишковість при кодуванні повідомлень, яка дозволяє контролювати і усувати помилки при передачі інформації по лініям зв’язку, а також між окремими пристроями цифрової обчислювальної системи. В цифрових обчислювальних машинах і системах широко використовується двійковий алфавіт, який має лише два символи - 0 і 1. Його використання спрощує технічну реалізацію пристроїв обчислювальної техніки.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Будь-яке дискретне повідомлення, сформульоване в деякому алфавіті, може бути переведено в двійковий алфавіт, якщо довжина двійкового слова відповідає формулі: $S_2 > S_1 \log_2 A_1$ (1.4)

Сучасні обчислювальні системи обробляють не тільки числову, але й текстову, інакше кажучи, алфавітно-цифрову інформацію, що містить цифри, букви, знаки розділення, математичні і інші символи.

Характер цієї інформації такий, що для її представлення потрібні слова змінної довжини. Використання для запису алгоритмів і автоматизація програмування алгоритмічних мов роблять необхідним введення в машину і виведення з неї, поряд з символами загального користування, ще й деяких спеціальних символів.

Ділова інформація в середньому містить вдвічі більше цифр, ніж букв. Тому поряд із загальною системою кодування алфавітно-цифрових символів ЕОМ зберігають також окрему систему кодування для десяткових цифрових даних.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Найбільше розповсюдження отримало **представлення інформації за допомогою восьмирозрядного складу, що називається байтом.**
За допомогою восьмирозрядного складу можна кодувати 256 різних символів. Декілька байтів утворюють слова.

ЕОМ виконує обробку інформації, що полягає в її запам’ятовуванні, передачі з одних пристроїв в інші, виконанні над інформацією арифметичних і логічних перетворень. Процес обробки інформації автоматизований за допомогою програмного управління. Програма є алгоритмом обробки інформації, і записується у вигляді послідовності команд, які повинні бути виконані машиною для отримання потрібного результату.

Натуральні форми представлення і натуральні одиниці інформації, що використовуються людиною при науково-технічних розрахунках, обробці економічної, планово-виробничої і іншої інформації, при програмуванні, істотно відрізняються від форм представлення і одиниць інформації в машині

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

З метою ознайомлення з систематизацією відомостей по кодуванню інформації в ЕОМ розглянемо **ієрархію <u>натуральних</u> і відповідних <u>машинних</u> одиниць інформації (в порядку зростання розмірів одиниць інформації):**

<u>Натуральні одиниці</u> інформації	**<u>Машинні</u>** одиниці інформації
Розряд	Розряд
Символ	Байт
Поле(число,реквізит)	Слово
Запис	Фраза
_____	Блок
Масив	Файл
_____	Том

Поле - <u>група символів, що мають певне значення і обробляються за одну й ту саму арифметичну чи логічну операцію.</u>

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Цьому визначенню відповідають: багаторозрядне число, команда, група символів, що позначають певну ознаку-реквізит якого-небудь об’єкту (наприклад, призвище чи рік народження деякої особи, назву деталі, її вагу і т. п.).

Запис - є групою полів, що описують ознаки (властивості, характеристики, параметри) деякого об’єкту. Наприклад рядок екзаменаційної відомості, наведений на рис. 1.3.

Кожен з реквізитів (ознак) - прізвище, номер залікової книжки і т.п. є полем. Поля об’єднані тим, що відноситься до певного студента.

Прізвище	№ залікової книжки	Дисципліна	Оцінка
Ващук	299156	ОТ	5

.

Рис. 1.3. Екзаменаційна відомість

Глава 1.
Предмет захисту

Масив - об’єднання записів, що описують деяку множину об’єктів (наприклад, екзаменаційні відомості чи їх сукупність).

Слово – група символів (розрядів) в пам’яті ЕОМ, що відповідає деякому полю. Термін машинне слово відносять до коду певної довжини, який зчитується з ОЗП чи записується в ОЗП за одне звертання. **Машинне слово** може бути двійковим числом з плаваючою чи фіксованою комою, командою, складатись з декількох складів (байтів). **Машинне слово** може також містити додаткові розряди (розряди контролю парності, розряди захисту пам’яті і інші). Звичайно машинне слово, зокрема команда, містить ціле число байтів.

Машинна одиниця інформації, що відповідає натуральній одиниці - запису, називається фразою (або також записом). Вона може займати декілька машинних слів. Блоком називають групу фраз (записів) розташованих компактно (без проміжків) на носії зовнішнього ЗП, яка може записуватись на носій з ОЗП, а також зчитуватись з носія в ОЗП одною командою.

Глава 1.
Предмет захисту

Серед натуральних одиниць інформації немає одиниці, що відповідає блоку. Місце в запам’ятовуючому пристрої, в якому зберігається група слів, що складають блок, називається зоною.

Інформаційному масиву відповідає машинна одиниця інформації - файл. **Файл** в загальному випадку складається з декількох блоків.

Том – машинна одиниця інформації, що відповідає пакету дисків

1.2. Процеси обробки інформації в АСОД

Інформаційні процеси в системах обробки даних типу автоматизованих систем управління (АСУ) можна умовно розділити на три групи:

1) інформаційно-довідникове забезпечення посадових осіб органів управління;
2) інформаційне забезпечення розрахункових задач;
3) обслуговування інформаційної бази АСУ.

Ці процеси реалізують посадові особи органів управління і обслуговуючий персонал АСУ з допомогою апаратних засобів автоматизації і зв’язку, програмного забезпечення і інформаційної бази АСУ.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

За ступенем стабільності інформацію поділяють на умовно-постійну і змінну. До умовно-постійної інформації відносять дані, які на протязі тривалого часу не змінюються. За використанням в процесах управління вся інформації поділяється на нормативну, довідникову, планову, оперативно-виробничу, звітну і аналітичну.

Опрацьована інформація видається посадовим особам безпосередньо на їх автоматизовані засоби управління і контролю (на пристрої друку і відображення індивідуального користування) або на пристрої видачі колективного користування.

На об`єкта АСУ накопичується і зберігається великий обсяг інформації , як документальної так і на
машинних носіях. Документальна інформація містить:

-відомості обліку документів, що зберігаються;
-табуляграми обліку інформації, що зберігається на машинних носіях;
-документи, що пройшли обробку на об’єкті АСУ;

Лекція 1
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.

Предмет захисту

Як було зазначено вище, в обчислювальних системах інформація представляється у двійковому алфавіті. Фізичними аналогами знаків цього алфавіту служать фізичні сигнали, що можуть приймати два стани, які можна чітко розрізнити. Обов’язковою вимогою до фізичних аналогів двійкового алфавіту є можливість надійного розпізнавання двох різних значень сигналів, які при описанні законів функціонування схем позначаються символами 0 і 1.

В схемах цифрових пристроїв змінні і відповідні їм сигнали змінюються і сприймаються не неперервно, а лише в дискретні моменти часу, що відповідають тактовим імпульсам.

В цифрових пристроях використовуються три способи фізичного представлення інформації: потенціальний, імпульсний і динамічний. Слово може бути представлене послідовним чи паралельним способом (кодом). Пристрої послідовної дії працюють повільніше, ніж паралельної. Однак пристрої паралельної дії вимагають більшого об’єму обладнання. В обчислювальній техніці використовують обидва способи в залежності від вимог, що ставляться до конкретного пристрою.

Лекція 1

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Інформація в обчислювальній системі підлягає різним процесам: введенню, зберіганню, обробці і виведенню.

Введення інформації в обчислювальну систему здійснюється з магнітних і оптичних носіїв інформації, клавіатури. мишок, сканерів. АЦП і т.п.

Зберігання інформації здійснюється на запам’ятовуючих пристроях: короткочасне - в ОЗП і в різних регістрах пам’яті, реалізованих на напівпровідникових пристроях, магнітних елементах; довготривале - в зовнішніх запам’ятовуючих пристроях, виконаних на магнітних і оптичних дисках і т.п.

На машинних носіях зберігаються:

-інформаційні масиви загального інформаційного поля;

-архівні дані;

-програмні блоки, файли, томи.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Інформаційні масиви загального інформаційного поля використовуються для видачі, за запитами, різних довідок, а також для інформаційного забезпечення розрахункових задач.

В склад архівних даних входить інформація, яка в даний момент не бере участь в роботі системи, але може бути використаною для відновлення чи заміни масивів, документування роботи системи і т.п.

Інформаційна єдність в АСУ забезпечується наступним шляхом:

-створення системи класифікації і кодування інформації;
-розробки і впровадження уніфікованих систем документації;
-уніфікації принципів побудови нормативів і їх відновлення;
-уніфікації системи показників для забезпечення співставлення в часі і за різними якісними і кількісними ознаками;
-регламентації потоків інформації за направленістю, об’ємом, періодичністю, достовірністю і терміновістю;

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

-уніфікація порядку формування і обробки даних.

Прикладом класифікації і уніфікації інформації може служити наведений на рис. 1.4. склад інформаційної бази АСУ.

Фізичне представлення інформації і процеси її обробки говорять про те, що реалізація системи захисту інформації повинна бути направлена також на захист апаратних і програмних засобів, в яких вона міститься, і які складають автоматизовану систему обробки даних. З цього випливає, що предметом захисту є тільки ресурси обчислювальної системи, як інколи вважають численні спеціалісти.

Під поняттям ресурси в широкому розумінні цього слова, розуміють запаси чого-небудь, можливості і т.п. В цьому змісті в обчислювальних системах під ресурсами розуміють програмні апаратні засоби обробки, зберігання і передачі інформації, яких може вистачити або не вистачити взагалі чи в даний момент часу. Тому поняття ресурси не може мати описані вище властивості інформації і деякі властивості засобів її обробки.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Як можна зауважити, предмет захисту в цьому випадку виходить за рамки цього поняття. Деякі спеціалісти відчули це і ввели поняття інформаційні ресурси, тим самим ще більш ускладнивши питання.

В буквальному змісті це поняття, із врахуванням сказаного вище, набуває значення інформаційних запасів. Інформація не матеріальна і не може бути витратним матеріалом (виключенням є запаси знань - але це зовсім інше поняття). Некоректність використання такого поняття очевидна.

Окрім того, інформація може бути захищена без апаратних і програмних засобів захисту з допомогою криптографічного перетворення. При цьому порушник має доступ до апаратних і програмних засобів, а до інформації доступу не має.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.

Предмет захисту

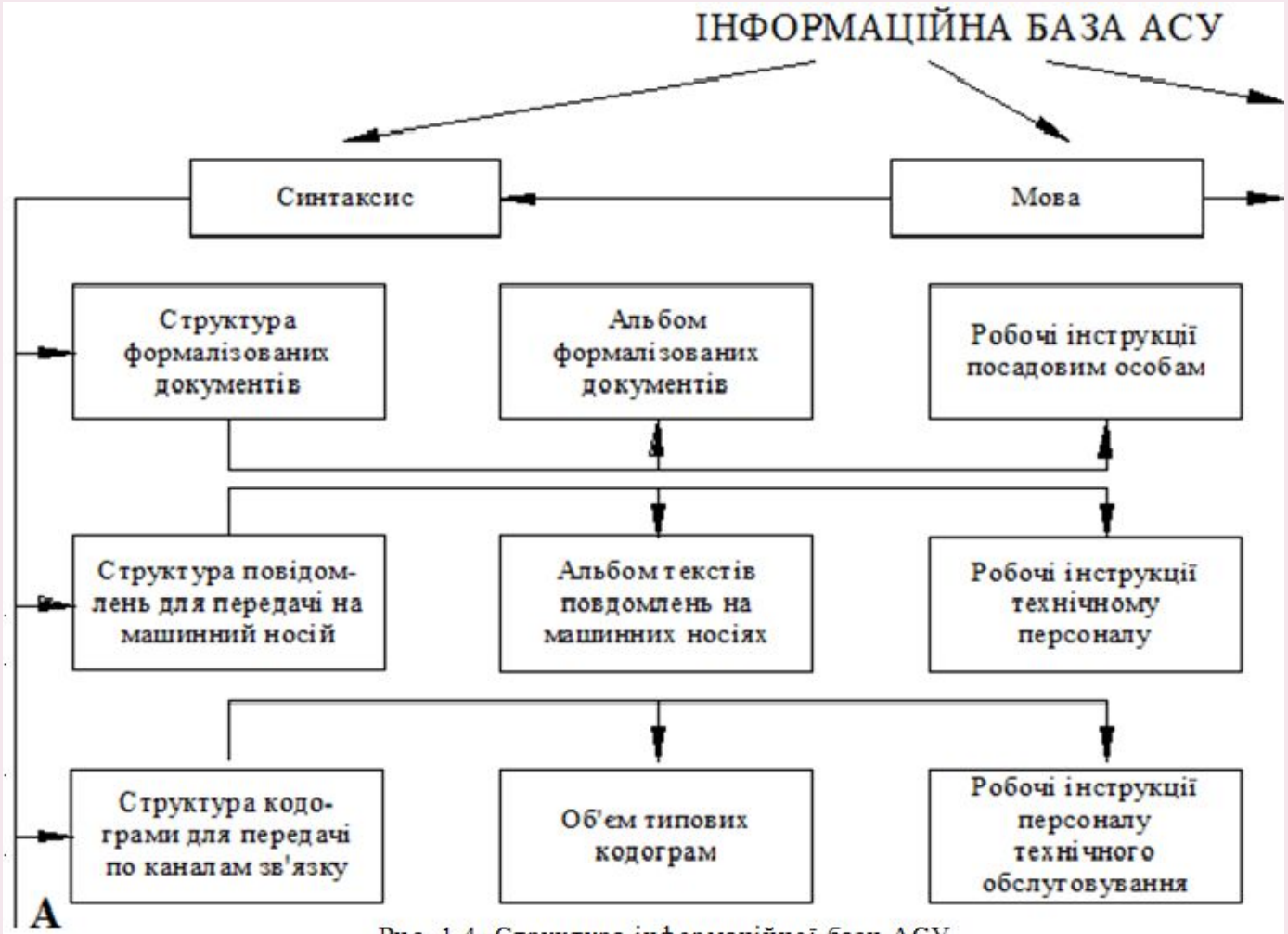


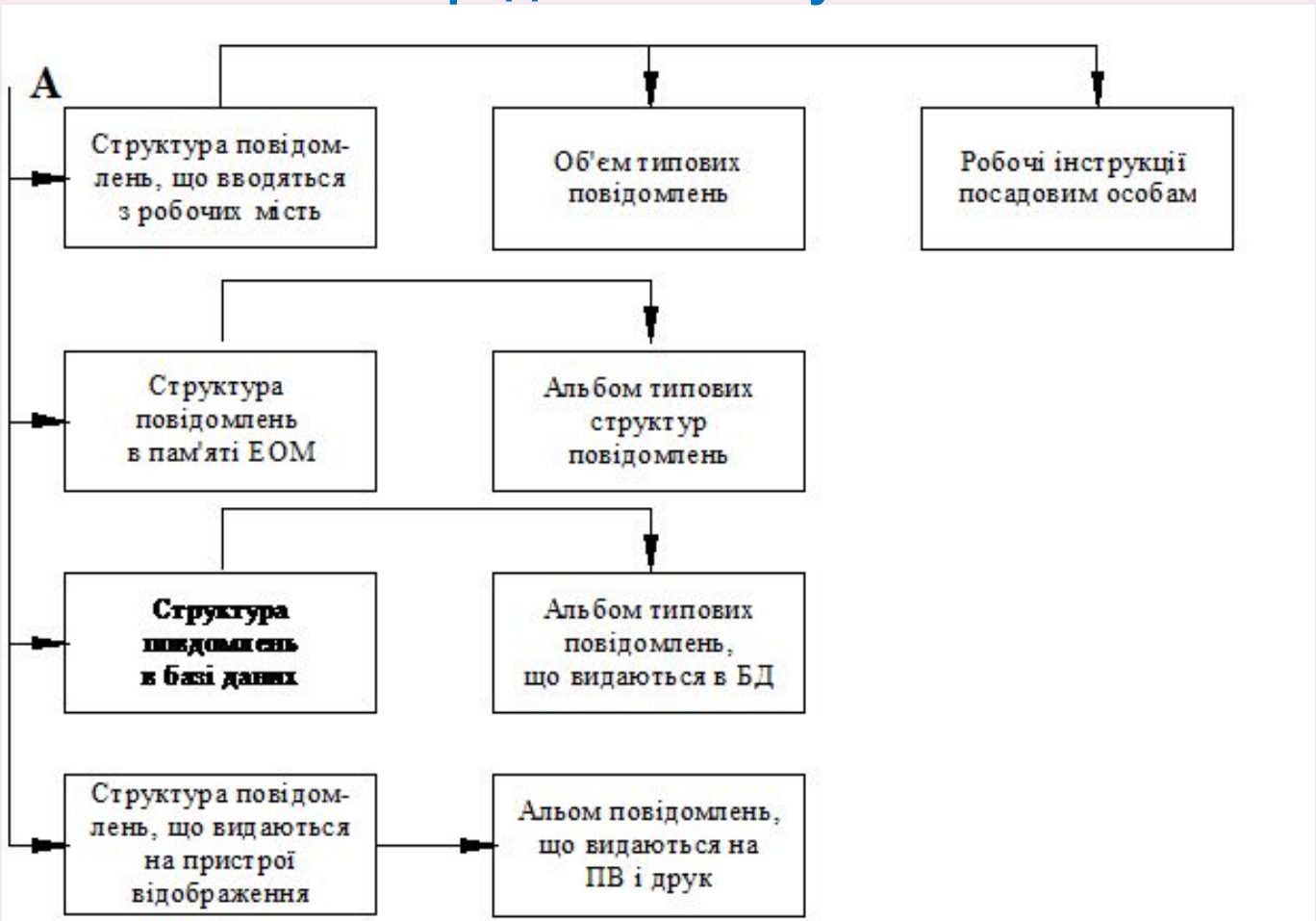
Рис. 1.4. Структура інформаційної бази АСУ

Лекція 1

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

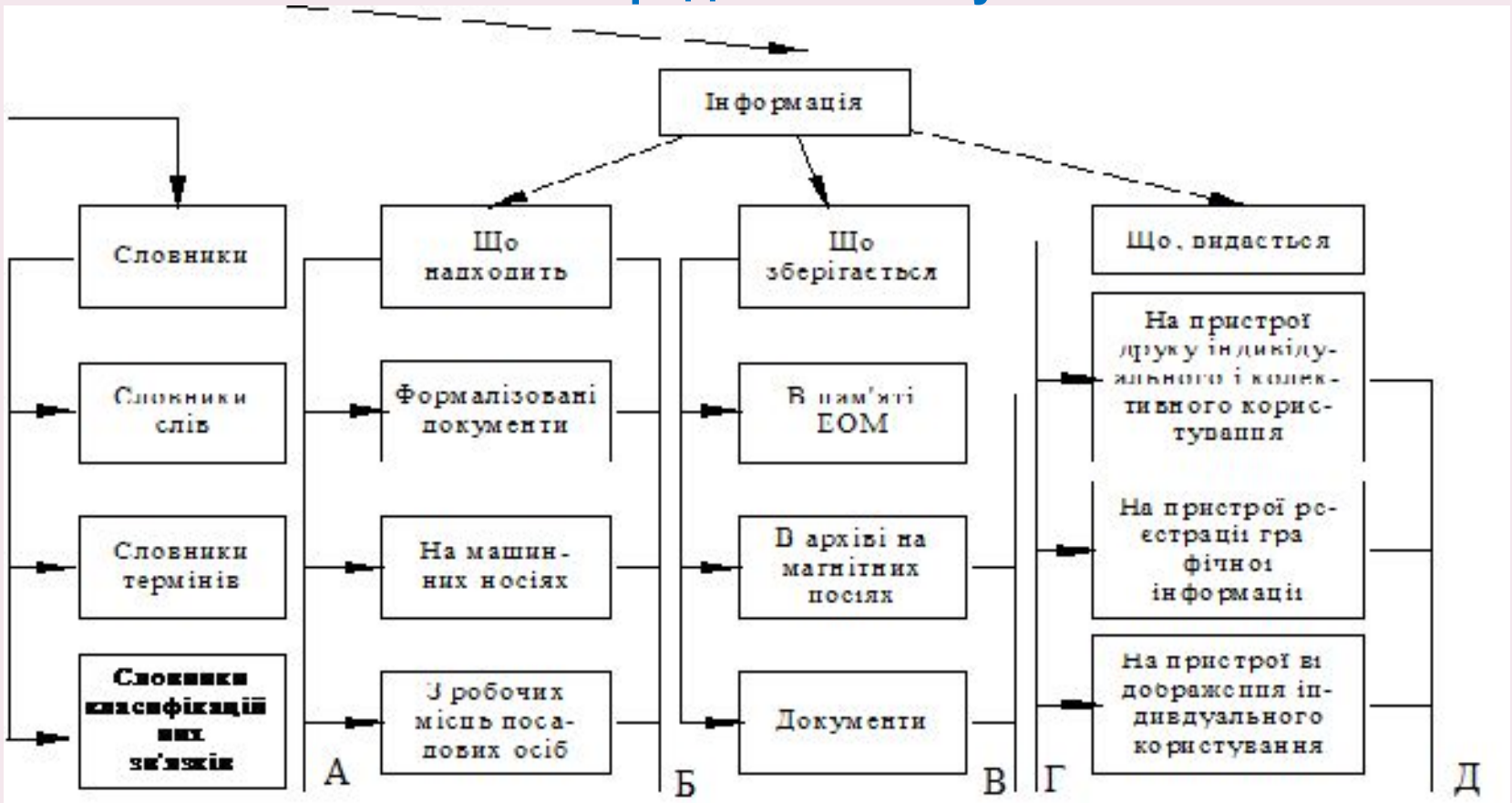


Продовження Рис.1.4

Лекція 1
Гарантоздатність автоматизованих систем

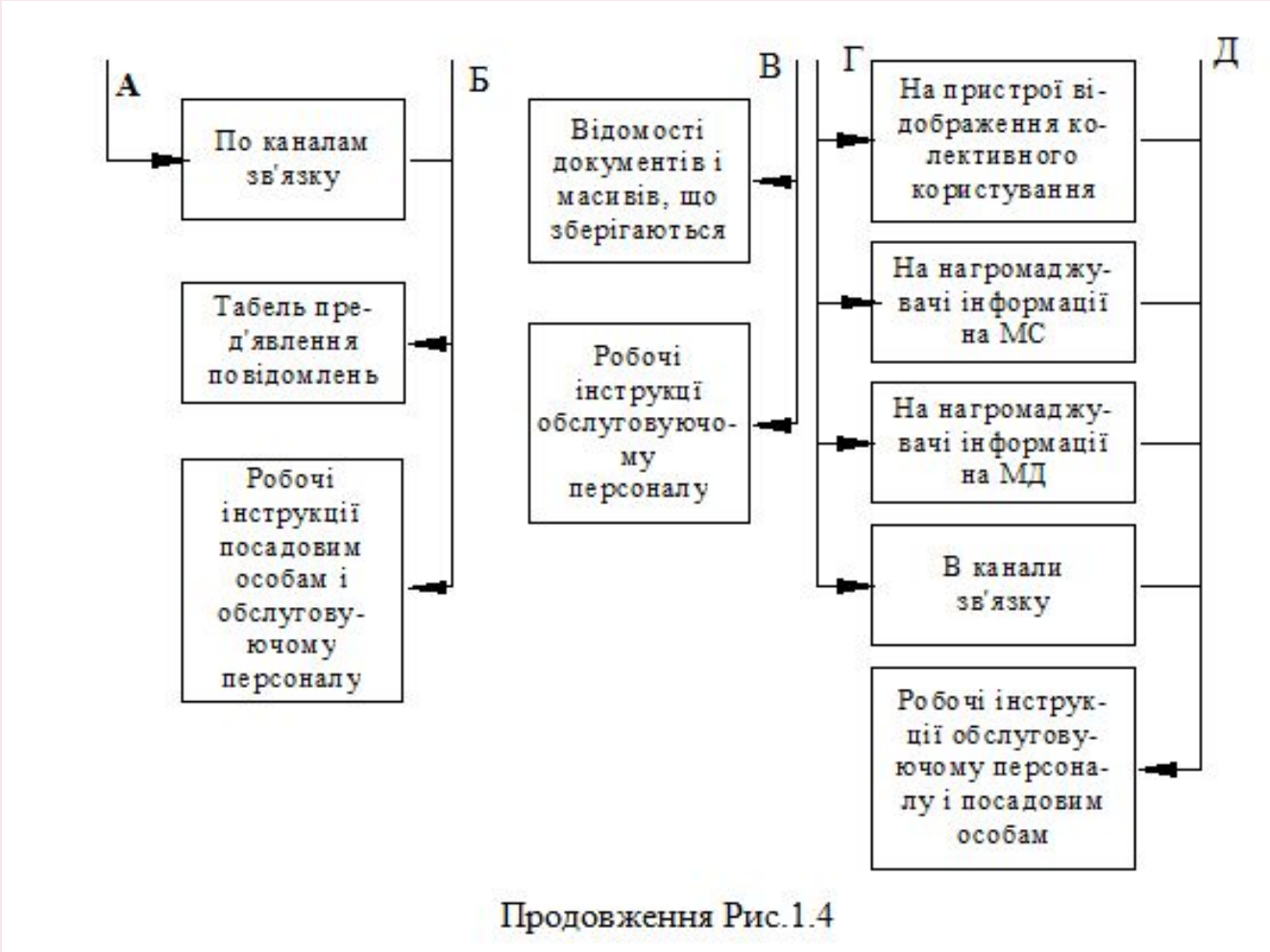
Глава 1.

Предмет захисту



Продовження Рис.1.4

Глава 1.
Предмет захисту



Продовження Рис.1.4

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.

Предмет захисту

1.3. Інформація як об’єкт права власності і як комерційна таємниця

Інформація - це предмет власності. Вона може бути власністю власника АСОД; власністю держави; тієї чи іншої організації, фірми, приватної чи суспільної; особистою власністю людини, що довірила її власнику АСОД. А там де є право власності, повинні бути чіткість, ясність і визначеність. Дотримання гарантій цих прав і забезпечує безпеку інформації.

По суті сфера безпеки інформації - не захист інформації, а захист прав власності на неї.

Розглянемо особливості інформаційної власності.

Історично традиційним об’єктом права власності є матеріальний об’єкт. Інформація не є матеріальним об’єктом, інформація - це знання, тобто відображення дійсності у свідомості людини (причому відображення істинне чи хибне - не суттєво, важливо, що в свідомості). В подальшому інформація може втілюватись в матеріальні об’єкти оточуючого нас світу.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Не будучи матеріальним об’єктом, інформація нероздільно зв’язана з матеріальним носієм: мозком людини чи відчуженим від людини матеріальним носієм, таким, як книга, дискета і інші види пам’яті (запам’ятовуючі пристрої).

З філософської точки зору, мабуть, можна говорити про інформацію як про абстрактну субстанцію, що існує сама по собі, але для нас ні зберігання, ні передача інформації неможливі без матеріального носія.

Як наслідок, інформація як об’єкт права власності може бути скопійована (тиражована) за рахунок матеріального носія. Матеріальний об’єкт права власності не копіюється. Дійсно, якщо розглянути дві однакові речі, то вони складаються з однакових структур, але матеріально різних молекул. А інформація при копіюванні залишається такою ж, це - те саме знання, та сама семантика. Переміщення матеріального об’єкту до іншого суб’єкту права власності неминуче і, як правило, спричиняє втрату цього об’єкту попереднім суб’єктом права власності, тобто відбувається очевидне порушення його прав власності.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту.

Небезпека копіювання і переміщення інформації ускладнюється тим, що вона, як правило, відчужена від власника, тобто зберігається і обробляється в сфері доступності великого числа суб’єктів, які не є суб’єктами права власності на цю інформацію. Це, наприклад, автоматизовані системи, в тому числі і мережі.

Розглянувши особливості інформації як об’єкту права власності, підкреслимо, що в іншому інформація, очевидно, нічим не відрізняється від традиційних об’єктів права власності.

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

Суб’єкт права власності на інформацію може передати частину своїх прав (розпорядження), не втрачаючи їх сам, другим суб’єктам, наприклад тому хто зберігає інформацію, тобто власнику матеріального носія інформації (це - володіння або користування) або користувачу (це - користування і, можливо, володіння).

Лекція 1
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Для інформації під правом розпорядження розуміється виняткове право (тобто ніхто інший, крім власника) визначати, кому ця інформація може бути надана (у володіння і користування).

Під правом володіння розуміється - мати цю інформацію в незмінному вигляді. Під правом користування розуміється право використовувати цю інформацію в своїх інтересах.

Таким чином, до інформації, крім суб’єкту права власності на цю інформацію, можуть мати доступ другі суб’єкти права власності як законно, санкціоновано (це - суб’єкти права на елементи власності), так і незаконно, несанкціоновано. Виникає складна система взаємовідношень між цими суб’єктами права власності.

Ці взаємовідносини повинні регулюватись і охоронятись, так як відхилення від них можуть привести до переміщення інформації, що спричиняє порушення права власності суб’єкту на цю інформацію. Іншими словами мова йде про реалізацію права власності на інформацію.

Лекція 1
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

Під цим будемо розуміти державну або приватну (чи державно-приватну) інфраструктуру, що запобігає порушенню права власності на інформацію. Виникає складна система взаємовідношень між цими суб’єктами права власності.

Ці взаємовідносини повинні регулюватись і охоронятись, так як відхилення від них можуть привести до переміщення інформації, що спричиняє порушення права власності суб’єкту на цю інформацію. Іншими словами мова йде про реалізацію права власності на інформацію. Під цим будемо розуміти державну або приватну (чи державно-приватну) інфраструктуру, що запобігає порушенню права власності на інформацію.

В принципі, як і для будь-якого об’єкту власності, така інфраструктура складається з ланцюга: законодавча влада - судова влада - виконавча влада (закон - суд - покарання).

Закон повинен передбачати відповідальність і повноваження суб’єктів права власності (на елементи власності).

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Кожний такий суб’єкт в рамках повноважень, що надані йому власником, несе перед ним відповідальність за передбачені законом і підтверджені судом перевищення цих повноважень, які привели чи могли привести до порушення права власності власника інформації.

Таким чином, не дивлячись на ряд особливостей, інформація поряд з традиційними матеріальними об’єктами може і повинна розглядатись законом як об’єкт права власності.

З огляду на перелічені вище особливості інформації як об’єкта права власності (здатність до копіювання, переміщення, відчуження) закон повинен регулювати відношення суб’єктів, а також суб’єктів і об’єктів права власності на інформацію з метою захисту прав як власника, так і законних володарів і користувачів інформації для захисту інформаційної власності від розголошення, витоку - несанкціонованого ознайомлення з нею, її обробки, зокрема копіювання, модифікації чи знищення.

Глава 1.
Предмет захисту

Під модифікацією інформації розуміють несанкціоновану її зміну, коректну по формі і складу, але іншу по змісту.

Таким чином можна визначити мету забезпечення безпеки інформації, що полягає в захисті прав власності на неї, і задачі безпеки інформації, які полягають в захисті її від витоку, модифікації і втрати.

Поняття ‘ комерційна таємниця’ введено в нашу практику з 1 січня 1991 р. статтею 33 закону

‘Про підприємства СРСР’, в якій сказано:

1. Під комерційною таємницею підприємства розуміють відомості, що не є державними секретами, пов’язані з виробництвом, управлінням, фінансами і іншою діяльністю підприємства, розголошення (передача, витік) яких може нанести шкоду його інтересам.

2. Склад і об’єм відомостей, що складають комерційну таємницю, визначається керівником підприємства.

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

Оскільки питання захисту державної таємниці добре розглянуті і на цей рахунок є достатньо багато матеріалів, доцільно приділити деяку увага питанню комерційної таємниці. Нижче наводяться пропозиції щодо її змісту для тих, хто вперше зустрічається з цією проблемою.

В наведеному нижче переліку відомості згруповані за тематичною ознакою. Запропоноване розділення на групи має характер рекомендації і може бути змінено в залежності від специфіки відомостей, що складають комерційну таємницю конкретного підприємства (організації). Відомості, що включені в даний перелік, можуть бути комерційною таємницею тільки з врахуванням особливостей конкретного підприємства (організації).

1. Відомості про фінансову діяльність:

-прибуток, кредити, товарообіг;
-фінансові звіти і прогнози;
-комерційні замисли;
-фонд заробітної плати;

Глава 1.
Предмет захисту

-вартість основних і обігових коштів;
-кредитні умови платежів;
-банківські рахунки;
-планові і звітні калькуляції.

2. Інформація про ринок:

-ціни, скидки, умови угод, специфікація продукції;
-об’єм, історія, тенденції виробництва і прогноз для конкретного продукту;
-ринкова політика і плани;
-маркетинг і стратегія цін;
-відношення із споживачами і репутація;
-чисельність і розміщення торгових агентів;
-канали і методи збуту;
-політика збуту;
-програма реклами.

Глава 1.
Предмет захисту

3. Відомості про виробництво і продукцію:
-відомості про технічний рівень, техніко-економічні характеристики виробів, що розробляються;
-відомості про планові терміни створення виробів, що розробляються;
-відомості про перспективні і сьогоднішні технології, технологічні процеси, методики і обладнання;
-відомості про модифікацію і модернізацію раніш відомих технологій, процесів, обладнання;
-виробничі потужності;
-стан основних і обігових фондів;
-організація виробництва;
-розміщення і розмір виробничих приміщень і складів;
-перспективні плани розвитку виробництва;
-технічні специфікації існуючої і перспективної продукції;
-схеми і креслення окремих вузлів, готових виробів, нових розробок;

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 1.
Предмет захисту

-відомості про стан програмного і комп’ютерного забезпечення;
-оцінка якості і ефективності;
-номенклатура виробів;
-спосіб упаковки;
-доставка.
4. Відомості про наукові розробки;
-нові технологічні методи, нові технічні, технологічні і фізичні принципи, що плануються до використання в продукції підприємства;
-програми НДР;
-нові алгоритми;
-оригінальні програми.
5. Відомості про систему матеріально-технічного забезпечення:
-відомості про склад торгових клієнтів, представників і посередників;
-потреби в сировині, матеріалах, комплектуючих вузлах і деталях, джерела задоволення цих потреб;
-транспортні і енергетичні по

Лекція 1
Гарантоздатність автоматизованих систем

Глава 1.
Предмет захисту

6. Відомості про персонал підприємства:
-чисельність персоналу підприємства;
-визначення осіб, що приймають рішення.
7. Відомості про принципи управління підприємством:
-відомості про перспективні і ті, що використовуються, методи управління виробництвом;
-відомості про факти ведення переговорів, тематику і мету нарад, засідань органів управління;
-відомості про плани підприємства щодо розширення виробництва;
-умови продажу і злиття фірм.
Існує також поняття банківської таємниці (БТ). Під БТ розуміють зобов’язання кредитної установи зберігати таємницю по операціям клієнтів, захист банківських операцій від ознайомлення з ними сторонніх осіб, перш за все конкурентів того чи іншого клієнта, таємницю по операціям, рахункам і вкладам своїх клієнтів і кореспондентів.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1 Актуальність застосування системної, нормативної, комплексної моделей захисту інформаційних технологій

Основою інформаційної безпеки інфраструктур суспільства та національної безпеки держави є – концепція технічного захисту інформації в Україні. Вирішення конкретної проблеми у відповідній предметній сфері потребує процедури управління. Наприклад, моніторинг параметрів екосистем навколишнього середовища за допомогою інформаційних систем координується управлінням на двох узгоджених рівнях – самого моніторингу, екологічної політики держави. Технічний захист інформації адекватно до потенційних загроз її безпеки, системи захисту має процедуру управління захистом, узгоджену з управлінням інформаційною безпекою на рівні державних інфраструктур.

Концепція об’єкт – загроза – захист – управління щодо безпеки ІТ має деякі аспекти. Розглянемо їх.

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Сьогодні провідними засобами розв’язання науково-технічних задач фундаментального та прикладного характеру є інформаційні, комунікаційні, інформаційно-комунікаційні технології. ***Інформаційна технологія*** – **це задана і керована процедура (конструктивний алгоритм) представлення інформаційних процесів (ІП) з використанням відповідних інформаційних ресурсів (ІР) та інформаційних систем (ІС). Безпеку ІТ *можна розглядати з позиції структури взаємозв’язку та взаємодії інформаційної технології і системи, інформаційних ресурсів і процесів, каналів зв’язку та каналів побічного електромагнітного випромінювання та наведення (КЗ/ КПЕМВН), елементів управління (У).*** Концепція безпеки ІТ і структура взаємозв’язку та взаємодії елементів знаходяться на рівні взаємовідношення. **Концепція проектується на структурі взаємозв’язку: ІТ та ІС; ІР та ІП; КЗ/ КПЕМВН та У** та формує безпеку ІТ: ***об’єкти захисту*** – ІР, ІС, ІП, КЗ/КПЕМВН, У; ***моделі загроз*** на рівні – ІР, ІС, ІП, КЗ/КПЕМВН; ***моделі захисту*** на рівні – ІР, ІС, ІП, КЗ/КПЕМВН; ***управління системою захисту*** на рівні – ІР, ІС, ІП, КЗ/КПЕМВН. алгоритмічних процедур (рис.1).

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

В цілому проблемі безпеки ІТ присвячується: розроблення законів і правил , нормативних документів ; діяльність технічних комітетів стандартизації; реалізація проектів програм наукових досліджень НАН України; написання фундаментальних монографій і прикладних наукових праць, в яких викладено усталені підходи, стандартизовані методології, проаналізовані моделі загроз та запропоновані моделі захисту даних в інформаційно-комунікаційних технологіях .

Застосування системної, нормативної, комплексної моделей захисту ІТ. ***Системна модель дає відповідь на запитання*** – що і як потрібно розробити для системи безпеки ІТ. ***Нормативна модель*** – на основі яких стандартів буде функціонувати ця система безпеки. ***Комплексна модель*** є підґрунтям для відповіді на запитання – чим реалізувати систему безпеки ІТ.

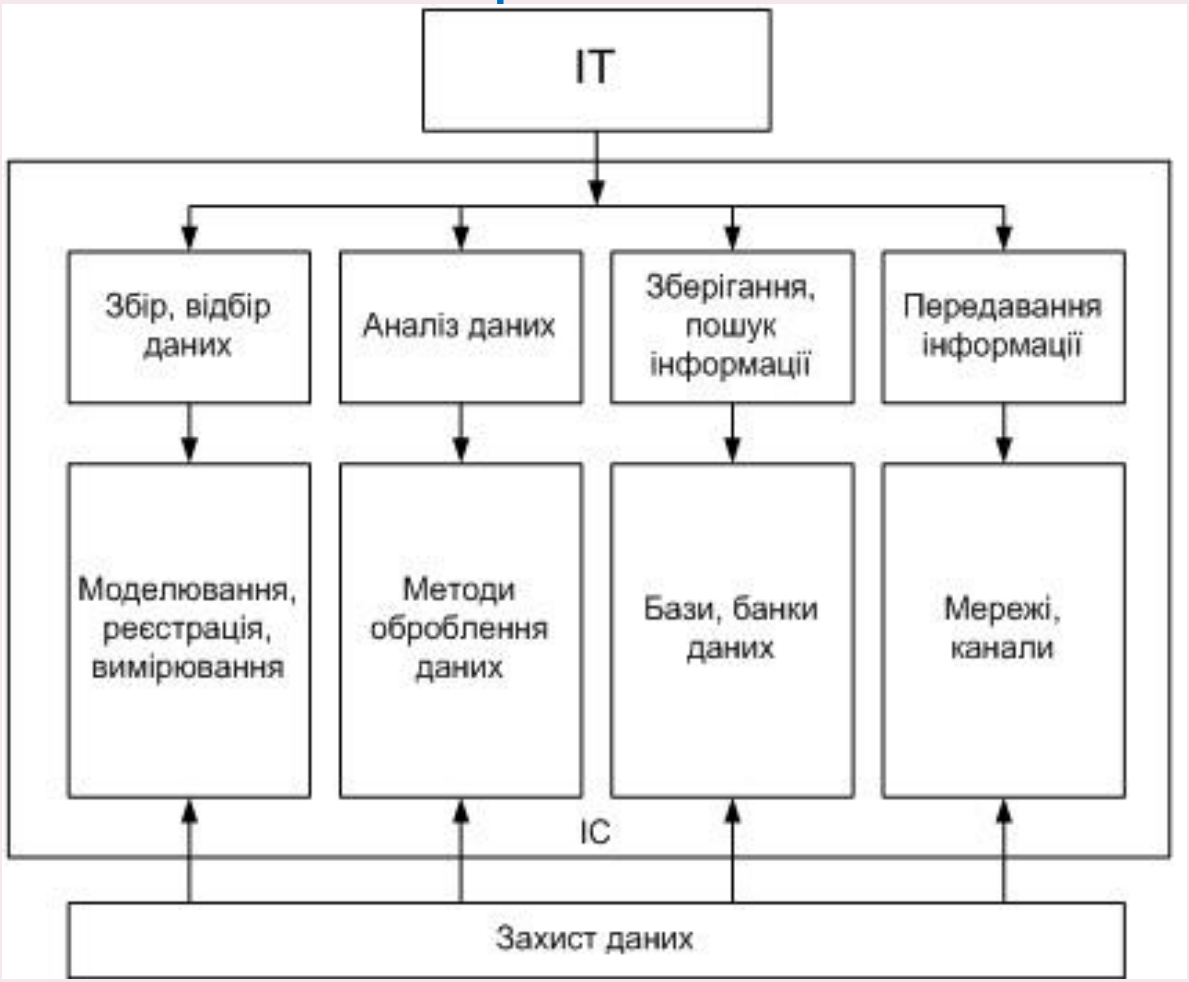
Лекція 2
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”

Кафедра захисту інформації

Глава 2

СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ



Лекція 2

Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.2 Системна модель захисту інформаційних технологій.

На основі принципів системного аналізу: цілісності, ієрархічності, структуризації пропонується системна модель захисту даних в інформаційних технологіях. ***Принцип цілісності*** – передбачає інтеграцію (об’єднання) частин цілого і проявляється в появі нових властивостей (ознак, параметрів, характеристик, фізичних величин) цілого, які відсутні у його частинах. ***Принцип ієрархічності*** – надає можливість точно виділити істотні властивості і взаємозв’язки складного об’єкта, що забезпечує докладний опис його властивостей за рахунок використання апріорних знань про внутрішню будову об’єкта. ***Принцип структуризації*** – вимагає розгляду об’єкта з різних точок зору з урахуванням взаємозв’язків виявлених аспектів. В основі такої моделі є концепція захисту даних: об’єкт – загроза – захист – управління. ***Системна модель захисту ІТ представлена у вигляді тривимірного простору x-y-z, охопленого сферою*** (рис.2).

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У площині x-z знаходяться об’єкти захисту: інформаційні ресурси, інформаційні системи, інформаційні процеси, канали зв’язку та канали побічного електромагнітного випромінювання і наведення, елементи управління. ***У площині y-z*** представлені рівні моделей загроз адекватно до об’єктів захисту, що у площині x-z. ***У площині x-y*** представлена система захисту інформаційних технологій (СЗІТ) адекватно до об’єктів захисту та моделей загроз. ***Стратегічна структура СЗІТ така***: засади – законодавчі, нормативно-методологічні, наукові; моделі захисту; напрямки; методології, способи, методи; засоби СЗІТ – технічні (апаратні, фізичні), програмні. *Подання об’єкта захисту* – інформаційних технологій п’ятьма взаємозв’язаними підсистемами: ІР; ІС; ІП; КЗ/ КПЕМВН; У дозволяє формувати моделі загроз для цих підсистем та відповідні моделі їх захисту на законодавчій, нормативній та науковій основах, не порушуючи концепції об’єкт – загроза – захист – управління для відповідного класу ІТ.

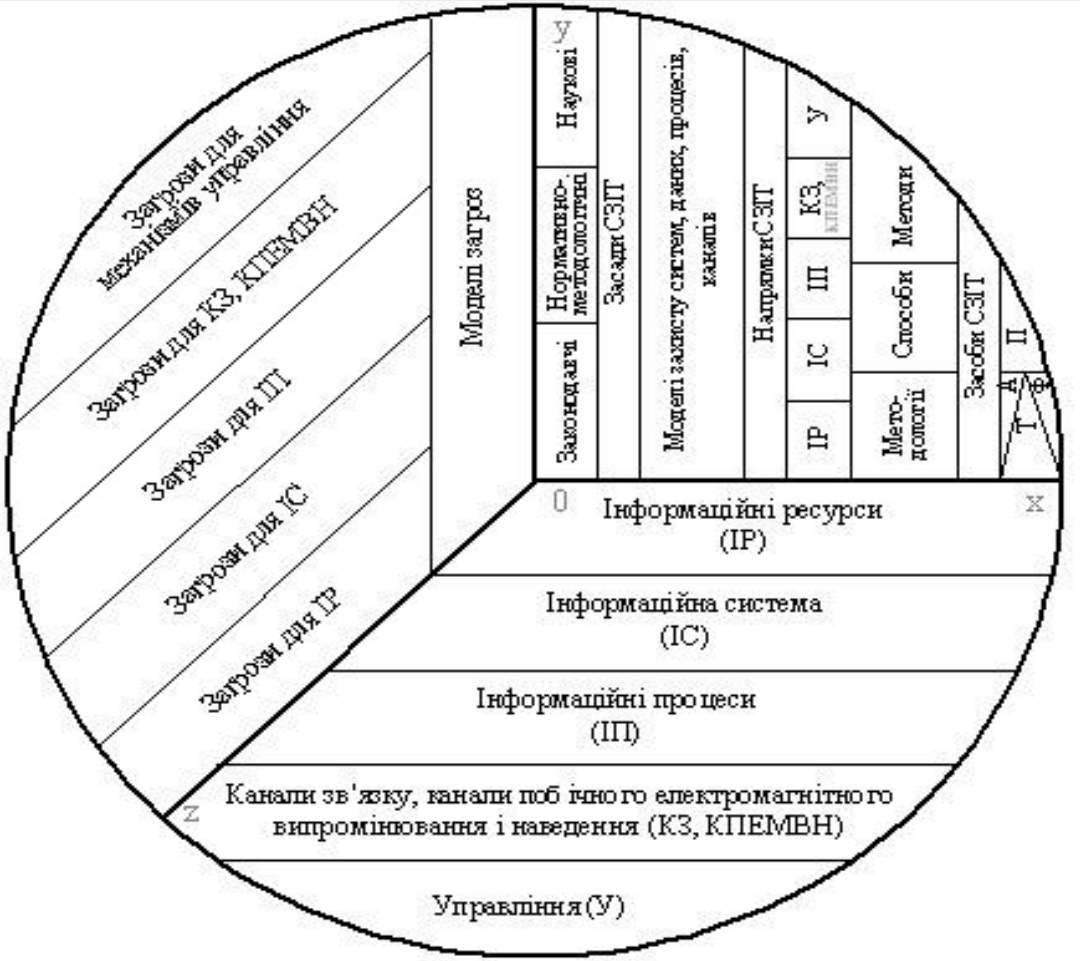
Лекція 2
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”

Кафедра захисту інформації

Глава 2

СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ



Лекція 2

Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вихідним аспектом забезпечення міцності комплексного захисту ІТ є – інформаційні ресурси, ступінь їх цінності та гриф таємності. **При створенні моделі загроз для ІТ необхідно враховувати такі елементи:**

– **загрози, як намір нанесення шкоди інформації** шляхом порушення її цілісності, конфіденційності або заволодіння нею у корисних цілях;

– **джерела загроз**, які класифікуються за природою виникнення: випадковість, навмисне заволодіння, нанесення шкоди інформації і т. і.;

– **цілі загроз**, *орієнтовані на такі ознаки інформації, як* ***конфіденційність, цілісність, доступність;***

– ***способи несанкціонованих дій (НСД)*** – підходи, які характеризують процес розглядання конкретної фізичної загрози для певного виду інформації. **Моделі захисту ІТ орієнтовані на:**

– **законодавчі, нормативно-методологічні, наукові засади**, які системно формують: основні принципи технічного захисту інформації, норми та вимоги, порядок проведення робіт та здійснення контролю його ефективності; концепції і моделі безпеки ІТ;

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

– **напрямок безпеки ІТ – ІР; ІС; ІП; КЗ/ КПЕМВН; У,** для кожного з яких обґрунтовуються критерії вибору (створення) методології, способу, методу, засобів СЗІТ з метою оптимізації проведення робіт із захисту даних;

– **технічні і програмні засоби захисту ІТ:** технічні пристрої – електричні, електромеханічні, електронні забезпечують секретність інформації, захист від модифікації, контроль даних; програмні засоби захисту – антивірусні програми, системи виявлення атак, контролери мережевого трафіку, комплексні системи захисту, програмні методи шифрування, методи маскування, автентифікації інформації, методи цифрового підпису т. і. забезпечують розмежування доступу та виключають несанкціоноване використання інформації.

Системна і нормативна моделі ***є підґрунтям для комплексної моделі захисту ІТ.***

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Комплексний захист ІТ від НСД до інформації та від її витоку можливими каналами на основі структури взаємозв’язку і взаємодії ІТ та ІС, ІР та ІП, КЗ та У здійснюється на рівнях: ***методологічного, апаратного-фізичного (технічного), програмного, комунікаційного, управлінського забезпечення***.

2.3 Нормативна модель захисту інформаційних технологій

Нормативна модель захисту ІТ *представлена у вигляді зрізаної піраміди, кожна сторона якої відповідає функціональним рівням системи захисту інформаційних технологій: А – методологічному, В – технічному (апаратному, фізичному, канальному), С – програмному, D – метрологічному* (рис.3).

Стандарти 1 – n є нормативною базою у сфері захисту ІТ згідно функціональних рівнів. До них відносяться: державні стандарти України **ДСТУ;** державні стандарти України, гармонізовані з міжнародними **ДСТУ ISO/IEC**; міждержавні стандарти **ГОСТ**; міждержавні, гармонізовані з міжнародними **ГОСТ Р ИСО/МЭК**; міжнародні стандарти **ISO** (Міжнародна організація зі стандартизації), **IEC** (Міжнародна електротехнічна комісія) (CEN, CENELEC, NIST, BSI)

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Методологічний рівень представляє підхід до захисту інформаційних технологій – концепції, моделі, методології захисту даних та управління захистом ІТ. ***Технічний*** **(апаратний, фізичний, канальний)** – апаратні пристрої, які впроваджені в апаратуру оброблення даних; пристрої, узгоджені з нею через інтерфейс; автоматичні пристрої і системи – елементи електронно-механічного обладнання охоронної сигналізації, замки т. і.; канали витоку інформації. ***Програмний рівень*** – це відповідно спеціалізовані програми, призначені для захисту ІТ. ***Метрологічний рівень*** розкривають елементи: метрологічної атестації, випробувань, стандартизації і сертифікації технічних і програмних засобів захисту інформації. Аспекти метрологічного рівня необхідно розглядати відповідно до нормативного документу , де окреслені етапи побудови системи захисту інформації в ІТ: визначення й аналіз загроз; розроблення системи захисту інформації; реалізація плану захисту інформації; контроль функціонування та керування системою захисту інформації.

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Реалізація цих етапів потребує: проведення метрологічної експертизи технічного завдання на розроблення системи захисту інформації; обґрунтування критеріїв вибору засобів вимірювальної техніки (ЗВТ), які комплектують систему захисту ІТ; розроблення рекомендаційних вимог до метрологічних характеристик ЗВТ, проведення метрологічної атестації (МА) ЗВТ; розроблення методик виконання вимірювань параметрів фізичних полів та сигналів з метою оцінювання імовірності витоку інформації технічними каналами та каналами спеціального впливу на систему; проведення МА системи захисту інформації згідно стандартизованих методик виконання вимірювань.

Лекція 2
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”

Кафедра захисту інформації

Глава 2

СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

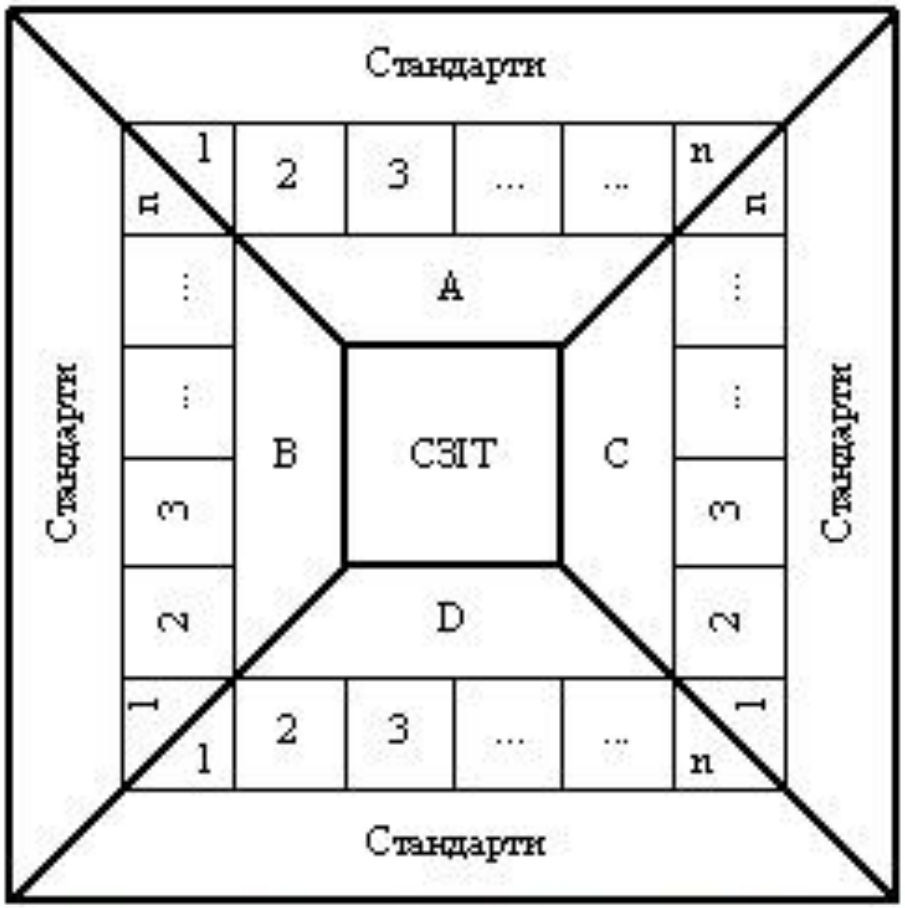


Рис. 3. – Нормативна модель захисту інформаційних технологій

Лекція 2

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Безпека ІТ представляє питання стандартизації та сертифікації засобів технічного захисту інформації. В цьому напрямі в Україні діють технічні комітети (ТК): **інформаційні технології (ТК-20)** з 1995 р., **технічний захист інформації (ТК-107)** з 2008 р. Серед основних елементів структури ТК-20: телекомунікації та обмін інформацією між системами; інженерія програмних засобів, автоматична ідентифікація та методи роботи з даними; управління даними та обмін; мови програмування та системний інтерфейс; коди та кодування інформації; оброблення, кодування та передавання звуків і зображень; методи та засоби безпеки в інформаційних технологіях; інформаційні та комунікаційні технології навчання; біометрія, мікропроцесорні системи; автоматизовані системи.

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.4 Комплексна модель захисту інформаційних технологій

Комплексна система захисту інформаційних технологій (КСЗІТ) представлена у вигляді ієрархічних сфер, в яких закладені п’ять рівнів захисту даних в ІТ (рис.4).

Першим рівнем КСЗІТ представлені самі об’єкти захисту – інформаційні ресурси; інформаційні системи; інформаційні процеси; канали зв’язку та канали побічного електромагнітного випромінювання і наведення, управління безпекою.

Другий рівень – підхід до захисту, що відображає застосування відповідних принципів захисту даних – *ступінь секретності інформації – **1**; апаратні та фізичні засоби захисту інформації – **2**; етапи життєвого циклу інформації в інформаційній системі – **3**; комплекс взаємозв’язку, взаємовідношення, взаємодії змінних в часі елементів, умов, факторів, які впливають на безпеку ІТ – **4**; елементи управління безпекою ІТ – **5**.*

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Третій рівень – КСЗІТ, представлена такими підсистемами захисту даних: *методологічною – **I**; технічною – **II**; програмною – **III**; комунікаційною – **IV**; управлінською – **V**.* Кожна підсистема КСЗІТ має відповідне нормативне забезпечення. Наприклад, рівень управлінського забезпечення захисту ІТ ґрунтується, зокрема на таких нормативних документах: - **ДСТУ ISO/IEC TR 13335-1** – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції й моделі безпеки ІТ

-**ДСТУ ISO/IEC TR 13335-2** – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ

-**ISO/IEC TR 13335-3** – Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ.

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Четвертий рівень – захисні пояси, які відображають характер захисту інформації: зовнішній пояс, який охоплює всю територію, де розташовані будівлі, що містять інформаційні технології – **α**; пояс будівель (приміщень), або пристроїв ІТ – **β**; пояс компонентів системи і технічних засобів, програмного забезпечення, елементів баз даних – **γ**; пояс технологічних процесів оброблення інформації (ввід, вивід, внутрішнє оброблення т. і.) – **θ.**

П’ятий рівень – комплекс методів і засобів протидії потенційним загрозам на рівні: виявлення – a; блокування – b; нейтралізації – c.

Національний університет “Львівська політехніка”
Кафедра захисту інформації
Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

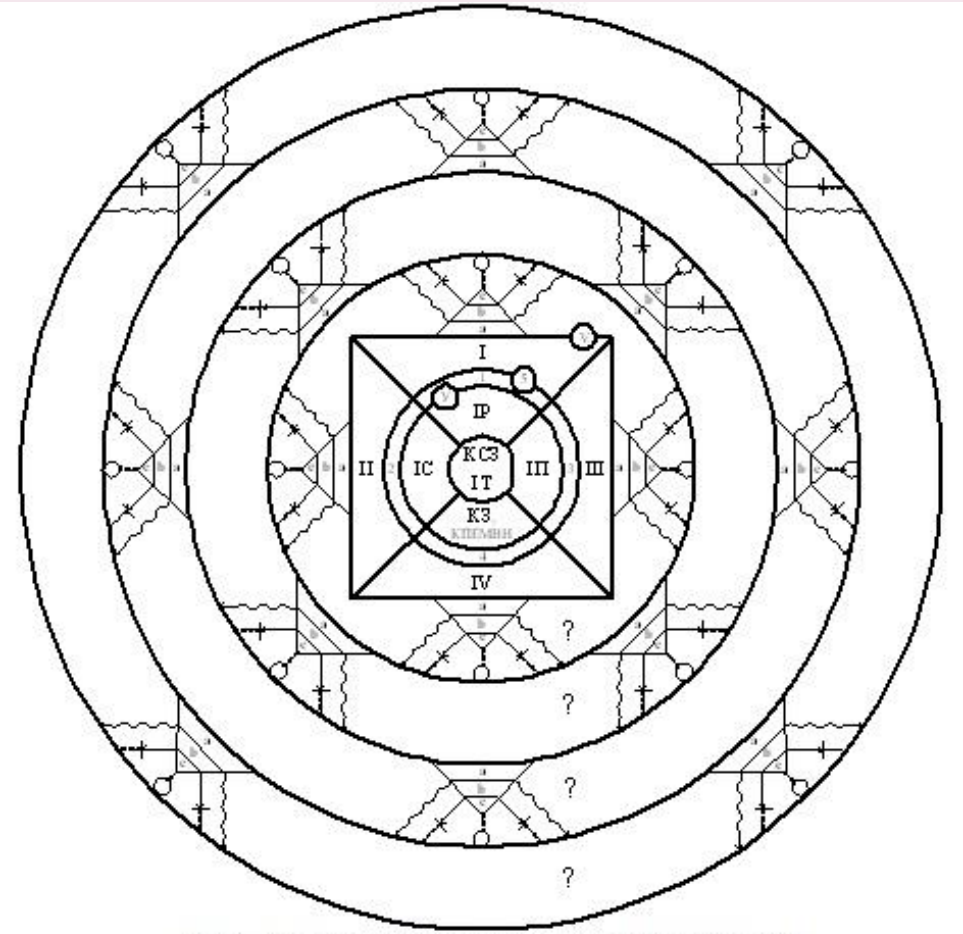


Рис. 4. – Комплексна модель захисту інформаційних технологій

Лекція 2
Гарантоздатність автоматизованих систем

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Висновки

1. Створена *системна модель* захисту ІТ *на основі концепції*: об’єкт – загроза – захист – управління дозволяє враховувати взаємозв’язок та взаємодію інформаційної технології і системи; інформаційних ресурсів і процесів; каналів зв’язку / каналів побічного електромагнітного випромінювання і наведення та елементів управління безпекою і, на цій основі, розробляти моделі загроз та адекватні до них моделі захисту.
2. Створена *нормативна модель* безпеки ІТ *на основі рівнів методологічного, технічного, програмного, метрологічного забезпечення* захисту даних, що дозволяє використовувати стандартизовані підходи, методології, способи, методи, засоби захисту ІТ або розробляти нові, уніфікувати їх на основі системної моделі та стандартизувати.

Глава 2
СИСТЕМНА, НОРМАТИВНА, КОМПЛЕКСНА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

3. *Комплексна модель* системи захисту ІТ *на основі п’яти рівнів безпеки*: *об’єкти захисту; підхід до захисту; підсистеми захисту; зовнішні і внутрішні пояси захисту; методи і засоби виявлення, блокування і повної нейтралізації загроз.* Модель дозволяє реалізувати на практиці систему безпеки ІТ на основі: ступеня цінності ІР, взаємозв’язку і взаємодії ІР, ІС, ІП, КЗ/ КПЕМВН, У, концепції об’єкт – загроза – захист – управління, тим самим забезпечити цілісність, конфіденційність і доступність інформації.

4. *Системна, нормативна, комплексна моделі* системи захисту ІТ впроваджені у сферу безпеки ІТ та ІКТ.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

3.1. Постановка задачі

Дослідження і аналіз багаточисельних випадків впливу на інформацію і несанкціонованого доступу до неї доводять, що їх можна розділити на ***випадкові і цілеспрямовані. Цілеспрямовані загрози*** часто шляхом їх систематичного використання ***можуть бути реалізовані через випадкові*** шляхом довготривалої масованої атаки несанкціонованими запитами чи вірусами. Наслідки, до яких призводить реалізація загроз: **1) руйнування (втрата)** інформації; **2) модифікація** (зміна інформації на хибну, яка коректна за складом і формою, але має інший зміст); **3) ознайомлення** з нею сторонніх осіб. Запобігання наведених наслідків в автоматизованій системі і є основною метою створення системи безпеки інформації. ***Для створення засобів захисту інформації необхідно визначити природу загроз, форми і шляхи їх можливого виникнення і здійснення в автоматизованій системі.***

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Для рішення поставленої задачі всю різноманітність загроз і шляхів їх впливу зведемо до простіших видів і форм, які були б адекватні їх множині в автоматизованій системі.

3.2. Випадкові загрози

Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем говорять про те, що на інформацію *в процесі введення, зберігання, виведення і передачі впливають різні випадкові загрози*. ***В результаті таких впливів на апаратному рівні відбуваються фізичні зміни рівнів сигналів в цифрових кодах, що несуть інформацію.***

При цьому спостерігаються *в одному, двох, трьох і т.д. розрядах* ***зміни 1 на 0 чи 0 на 1,*** *чи те і друге разом, але в різних розрядах*, *наслідком чого в результаті є зміна значення коду на інший.*

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Якщо ***засоби функціонального контролю***, що використовуються для цієї мети, здатні виявити ці зміни (наприклад, контроль за модулем 2 легко виявляє однократну помилку), виконується бракування даного коду, а пристрій, блок, модуль чи мікросхема, що беруть участь в обробці, оголошуються несправними. *Якщо* ***функціональний контроль відсутній*** *чи нездатний виявити несправність на даному етапі обробки, процес обробки продовжується по хибному шляху, тобто відбувається модифікація інформації*. ***В процесі подальшої обробки в залежності від змісту і призначення хибної команди*** можливі або передавання інформації за хибною адресу, або передавання хибної інформації адресату, або стирання чи запис іншої інформації в ОЗП чи ПЗП, тобто ***виникають небажані події: 1) руйнування (втрата), 2) модифікація, 3) витік інформації.***

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

На програмному рівні в результаті випадкових впливів може відбутись зміна алгоритму обробки інформації на непередбачений, характер якого теж може бути різним: 1) зупинка обчислювального процесу; 2) модифікація обчислювального процесу. Якщо засоби функціонального контролю не виявляють зміни алгоритму: 1) наслідки модифікації алгоритму (даних) можуть бути невиявленими чи призвести також до руйнування інформації; 2) при зміні адреси пристрою - до витоку інформації. При програмних помилках можуть підключатись програми введення/виведення і передавання їх на заборонені пристрої.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Причинами випадкових впливів при експлуатації автоматизованої системи можуть бути:

-відмови і збої апаратури;
-завада в лініях зв’язку від впливів зовнішніх факторів;
-помилки людини, як складової системи;
-схемні і системотехнічні помилки при проектантуванні;
-структурні, алгоритмічні і програмні помилки;
-аварійні ситуації та інші впливи.

Частота відмов і збої апаратури збільшуються при виборі і проектуванні системи, що є слабою у відношенні надійності функціонування апаратури. Завади в лініях зв’язку залежать від правильності вибору місця розташування технічних засобів АСОД відносно один одного і по відношенню до апаратури і агрегатів сусідніх автоматизованих систем.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

При розробці складних автоматизованих систем збільшується число схемних, схемотехнічних, структурних, алгоритмічних і програмних помилок. На їх кількість в процесі проектування великий вплив мають факторіи: класифікація проектантів, умови їх роботи, наявність досвіду т.і.

На етапі виготовлення і випробувань на якість апаратури, що входить в АСОД, впливають повнота і якість документації, за якою її виготовлюють, технологічна дисципліна і інші фактори.

До помилок людини, як ланки системи, слід віднести: 1) помилки людини, як джерела інформації, людини-оператора; 2) неправильні дії обслуговуючого персоналу; 3) помилки людини, як ланки, що приймає рішення.

Помилки людини: 1) логічні (неправильно прийняті рішення), 2) сенсорні (неправильне сприйняття оператором інформації), 3) оперативні, чи моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатись в межах: від 1 - 2 % до 15 - 40 %

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Хоча ***людина як елемент системи*** має у порівнянні з технічними засобами ряд переваг (здатність адаптуватись, навчатись; еврістичність; вибірковість; здатність до роботи в конфліктних ситуаціях), вона в той самий час має ряд недоліків, основними з яких є: ***втомлюваність, залежність психологічних параметрів від віку, чутливість до змін параметрів оточуючого середовища, залежності якості роботи від фізичного стану, емоційність***.

Не мале значення мають також помилки людини, як ланки системи, що приймає рішення. Особливо важливе значення проблема боротьби з помилками такого характеру набуває в автоматизованих системах управління адміністративного типу.

Помилки людини як ланки системи, що приймає рішення, визначаються не повною адекватністю уявлення людини про реальну ситуацію і властивістю людини з наперед визначеною позицією діяти за раніш наміченою програмою.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Наприклад, керівник, будучи наперед впевненим, що майстер завищив кількість потрібного дефіцитного матеріалу, зменшує відповідну заявку і тим самим вводить в АСУ помилкові дані.

Другою важливою особливістю людини є прагнення до побудови спрощеної моделі ситуації, що розглядається. Неправильне спрощення конкретної ситуації, виключення з неї важливих моментів і прийняте при цьому рішення можуть виявитись помилковими.

До загроз випадкового характеру слід також віднести аварійні ситуації, які можуть виникнути на об’єкті розміщення автоматизованої системи. ***До аварійних ситуацій відносяться:***

- ***відмова функціонування АСОД в цілому***, наприклад, вихід з ладу електроживлення і освітлення;
- ***стихійні лиха***: пожар, повінь, землетрус, урагани, удари блискавки, обвали іт. п.;
- ***відмова систем життєзабезпечення*** на об’єкті експлуатації АСОД.

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

3.3. Цілеспрямовані загрози

Цілеспрямовані загрози пов’язані з діями людини, причинами яких можуть бути певні невдоволення своєю життєвою ситуацією, чисто матеріальний інтерес чи проста розвага з самоствердженням, як у хакерів і т.і.

Задача забезпечення безпеки - ***запобігання, виявлення і блокування*** його можливих дій в АСОД. Потенційні загрози з цієї сторони розглядаються тільки в технічному аспекті.

Для того щоб поставити задачу більш конкретно проаналізуємо об’єкт захисту інформації на предмет введення-виведення, зберігання і обробки інформації і можливостей порушника по доступу до інформації при відсутності засобів захисту в даній автоматизованій системі.

В якості об’єкту захисту виберемо обчислювальну систему, *яка може бути 1) елементом обчислювальної мережі; 2) великої АСУ.*

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Для обчислювальної системи ***в цьому випадку характерні наступні штатні (законні) канали доступу до інформації:***

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

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

За відсутності захисту порушник може використати як штатні, так і інші фізичні канали доступу – ***можливі канали несанкціонованого доступу (МКНСД) в обчислювальній системі***, через які можливе отримання доступу до апаратури, програмного забезпечення і здійснення крадіжки, руйнування, модифікації інформації і ознайомлення з нею. **До МКНСД відносять**:

-усі перелічені вище ***штатні засоби при їх використанні законними користувачами не по незнанню*** і за межами своїх повноважень;

-усі перелічені вище ***штатні засоби при їх використанні сторонніми особами***;

- технологічні пульти управління;

-внутрішній монтаж апаратури;

-лінії зв’язку між апаратними засобами даної обчислювальної системи;

-побічне електромагнітне випромінювання інформації з апаратури системи;

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

-побічні наводки інформації по колу електроживлення і заземлення апаратури;
-побічні наводки інформації на допоміжних сторонніх комунікаціях;
-відходи обробки інформації у вигляді паперових і магнітних носіїв в корзині.

Для автоматизованої обробки інформації з централізованою обробкою даних характерні такі способи НСД:

1) **за відсутності законного користувача, контролю і розмежування доступу до терміналів** кваліфікований порушник легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом введення відповідних запитів/команд.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

2) **за наявності вільного доступу в приміщення** можна візуально спостерігати інформацію на засобах відображення і документування., а на останніх вкрасти паперові носії, зняти зайву копію, а також вкрасти інші носії з інформацією: магнітні стрічки, диски і т.і.; **3) особливо небезпечним є безконтрольне завантаження програмного забезпечення в ЕОМ**, в якому можуть бути змінені дані, алгоритми чи введена програма “троянський кінь” - програма, що виконує додаткові незаконні функції: запис інформації на сторонній носій, передачу в канали зв’язку другому абоненту обчислювальної мережі, внесення в систему комп’ютерного вірусу і т.і.; **4) за відсутності розмежування і контролю доступу до технологічної і оперативної інформації** можливий НСД до оперативної інформації зі сторони терміналу функціонального контролю; **5) небезпечною є ситуація, коли порушником є користувач обчислювальної системи, який за своїми функціональними обов’язками має законний доступ** до однієї частини інформації, а звертається до другої за межами своїх повноважень.

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Зі сторони законного користувача існує багато способів як порушити роботу обчислювальної системи, зловживати нею, добувати, модифікувати чи знищувати інформацію.

Для цієї мети можуть бути використані привілейовані команди введення/виведення, відсутність контролю законності запиту і звертань до адрес пам’яті ОЗП, ПЗП і т.і. При неоднозначній ідентифікації ресурсів порушник може подавити системну бібліотеку своєю бібліотекою, а модуль, що завантажується з його бібліотеки, може бути введений в супервізорному режимі. Вільний доступ дозволяє йому звертатись до чужих файлів і банків даних і змінювати їх випадково чи цілеспрямовано.

При технічному обслуговуванні (профілактиці чи ремонті) апаратури можуть бути виявлені залишки інформації на магнітній стрічці, поверхні дисків і других носіях інформації. Стирання інформації звичайними методами при цьому не завжди ефективно. Її залишки можуть бути зчитаними.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

При транспортуванні носія по території, що не охороняється, існує небезпека його перехоплення з наступним ознайомленням сторонніх осіб з секретною інформацією.

Не має змісту створювати системи контролю і розмежування доступу до інформації на програмному рівні, якщо не контролюється доступ до пульта управління ЕОМ, внутрішнього монтажу апаратури, кабельним з’єднанням.

1) Порушник може стати законним користувачем системи в режимі розділення часу, визначивши порядок роботи законного користувача або працюючи вслід за ним по одним і тим самим лініям зв’язку. *2) Порушник може використати метод проб і помилок* і реалізувати дірки в операційній системі, прочитати паролі. *3) Без знання паролів порушник може здійснити селективне включення в лінію зв’язку* між терміналом і процесором ЕОМ. *4) Без переривання роботи законного користувача може продовжити її від його імені*, відмінивши сигнали відключення законного користувача.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Процеси обробки, передавання і зберігання інформації апаратними засобами автоматизованої системи забезпечуються спрацюванням логічних елементів, побудованих на базі напівпровідникових приладів, які частіш за все реалізовані у вигляді інтегральних схем.

Спрацювання логічних елементів зумовлено високочастотною зміною рівнів напруг і струмів, що призводить до виникнення в ефірі, колах живлення і заземлення, а також в паралельно розташованих колах і індуктивностях сторонньої апаратури, електромагнітних полів і наводок, які несуть в амплітуді, фазі і частоті своїх коливань ознаки інформації, що обробляється.

Дії порушника: *1) **Використання порушником різноманітних приймачів може призвести до їх приймання і витоку інформації**. Із зменшенням відстані між приймачем порушника і апаратними засобами імовірність прийому сигналів такого характеру збільшується.*

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

2) ***Безпосереднє підключення порушником приймальної апаратури*** *і спеціальних датчиків до кіл електроживлення і заземлення,* ***до каналів зв’язку*** *також дозволяє здійснювати несанкціоноване ознайомлення з інформацією, а несанкціоноване підключення до каналів зв’язку передавальної апаратури може привести і до модифікації інформації.*

3) ***Особливо слід зупинитись на загрозах, що впливають на канали і лінії зв’язку обчислювальної мережі.***

Допустимо, що порушник може розташовуватись в деякій точці мережі, через яку повинна проходити вся інформація, що його цікавить. Зокрема, **в міжмережевих умовах порушник може прийняти вигляд шлюзу в деякій проміжній мережі**, яка забезпечує єдиний шлях з’єднання між двома процесорами, що є кінцями з’єднання, яке цікавить порушника, так як це показано на рис. 3.2.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

В цьому випадку, не дивлячись на те, що мережа-джерело (А) і мережа адресат (Г) захищені, порушник може діяти на з’єднання, оскільки воно проходить через шлюз, що з’єднує мережі Б і В. *Порушник може займати позицію, що дозволяє здійснювати: 1) пасивне і 2) активне перехоплення.*

1) **У випадку пасивного перехоплення** *порушник тільки слідкує за повідомленнями, що передаються по з’єднанню, без втручання в їх потік.* ***Спостереження порушника за даними (прикладного рівня) в повідомленні дозволяє розкрити зміст повідомлень***. Дії порушника: 1) *Порушник може також* ***слідкувати за заголовками повідомлень***, навіть якщо дані не зрозумілі йому, з метою визначення місця розміщення і ідентифікаторів процесів, що беруть участь в передачі даних. 2) *Порушник може* ***визначити довжини повідомлень і частоту їх передавання*** *для визначення характеру даних, що передаються, тобто* ***провести аналіз потоку повідомлень***.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 3.

ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

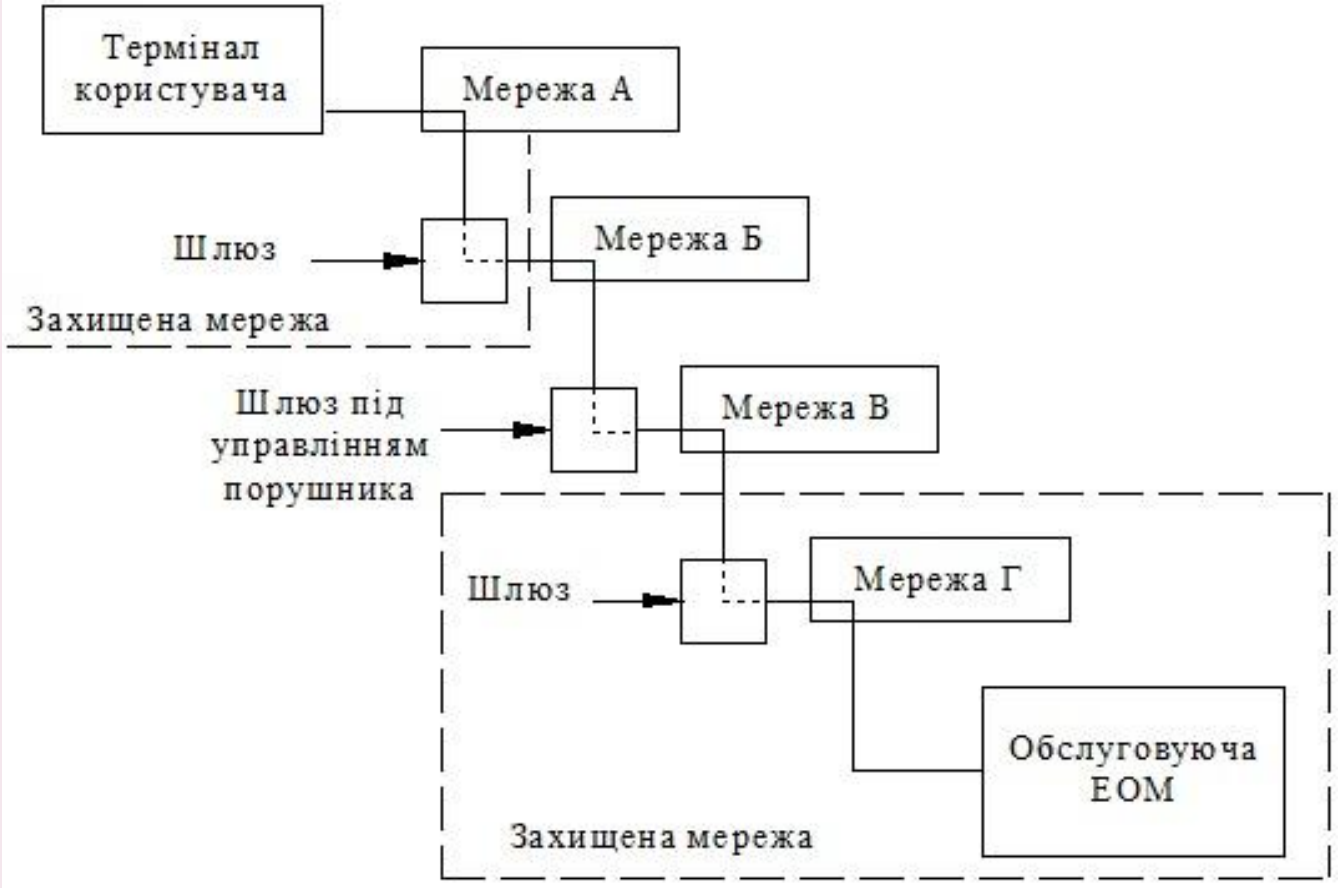


Рис. 3.2. Схема можливого підключення порушника до обчислювальної мережі

Лекція 3

Гарантоздатність автоматизованих систем

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

2) Порушник може також займатись активним перехопленням, виконуючи різні дії над повідомленнями, що передаються по з’єднанню. **Ці повідомлення можуть бути:** *1) вибірково змінені, 2) знищені, 3) затримані, 4) переупорядковані, 5) продубльовані і введені в з’єднання в більш пізній момент часу.*

Порушник може створювати фальшиві повідомлення і вводити їх в з’єднання. ***Ці дії можна визначити, як зміну потоку і змісту повідомлень***.

Крім того, порушник може скидати всі повідомлення чи затримувати їх. Ці дії можна класифікувати, як переривання процесу передавання повідомлень.

Спроба використовування запису попередніх послідовностей повідомлень по ініціюванню з’єднань класифікується, як ініціювання хибного з’єднання.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

При цьому розглядались не тільки можливості порушника, що отримав законний доступ до обладнання мережі, але й впливи, обумовлені помилками програмного забезпечення чи властивостями протоколів мережі, що використовуються. **Сформульовано *п’ять основних категорій загроз безпеці даних в обчислювальних мережах:***

1) *розкриття змісту повідомлень*, що передаються;
2) *аналіз трафіку*, що дозволяє визначити належність відправника і одержувача даних до однієї з груп користувачів мережі, пов’язаних спільною задачею;
3) *зміна потоку повідомлень*, що може привести до порушення режиму роботи якого-небудь об’єкту, що управляється з віддаленої ЕОМ;
4) *неправомірна відмова в наданні послуг*;
5) *несанкціоноване встановлення зв’язку*.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Дана класифікація не суперечить визначенню терміну “безпека інформації” і поділу потенційних загроз на: *витік, модифікацію і втрату інформації*. ***Загрози 1 і 2*** *можна віднести до витоку інформації*, ***загрози 3 і 5*** *- до її модифікації*, а ***загрозу 4 -*** *до порушення процесу обміну інформацією, тобто до її втрати для одержувача.* ***В обчислювальних мережах порушник може використовувати наступні стратегії поведінки:***

1) отримати несанкціонований доступ до секретної інформації;
2) видати себе за іншого користувача, щоб зняти з себе відповідальність або ж використати його повноваження з метою формування неправдивої інформації, зміни законної інформації, використання фальшивого посвідчення особи, санкціонування удаваних обмінів інформацією або ж їх підтвердження;
3) відмовитись від факту формування інформації, що була передана;
4) стверджувати те, що інформація отримана від деякого користувача, хоча насправді вона сформована самим порушником;

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

5) стверджувати те, що користувачу в певний момент часу була надіслана інформація, яка насправді не надсилалась (чи надсилалась в інший момент часу);
6) відмовитись від факту отримання інформації, яка насправді була отримана, чи стверджувати про інший час її отримання;
7) незаконно розширити свої повноваження стосовно доступу до інформації і її обробки;
8) незаконно змінити повноваження других користувачів (розширити чи обмежити, вивести чи ввести других осіб);
9) приховати факт наявності деякої інформації в іншій інформації (прихована передача одної в змісті іншої інформації);
10) підключитись до лінії зв’язку між другими користувачами в якості активного ретранслятора;
11) вивчити, хто, коли і до якої інформації отримує доступ (навіть, якщо сама інформація залишається недоступною);

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

12) заявити про сумнівність протоколу забезпечення інформацією через розкриття деякої інформації, яка згідно умовам протоколу повинна залишатись секретною;
13) модифікувати програмне забезпечення шляхом вилучення чи добавлення нових функцій;
14) цілеспрямовано змінити протокол обміну інформацією з метою його порушення чи підриву довіри до нього;
15) завадити обміну повідомленнями між другими користувачами шляхом введення завад з метою порушення автентифікації повідомлень.

Аналіз останніх можливих стратегій порушника в обчислювальній системі говорить про те, наскільки важливо знати, кого рахувати порушником. При цьому в якості порушника розглядається не тільки стороння особа, але й законний користувач. З цих позицій наведені вище п’ять видів загроз характерні для поведінки стороннього порушника.

Глава 3.
ПОТЕНЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В АСОД

Тоді з числа останніх загроз можна віднести до п’яти згаданих вище видів наступні загрози: 1, 10, 11, 15.

Аналіз останніх загроз свідчить про те, що задачу захисту від них можна умовно розділити на задачі двох рівнів: **1) користувачів і 2) елементів мережі, з якими працюють користувачі мережі.**

До рівня елементів мережі віднесяться загрози: 2, 7, 8, 13 і 14.

Рівень взаємовідносин користувачів називається рівнем довіри одного користувача до іншого. Для забезпечення гарантій цієї довіри потрібні спеціальні засоби і критерії оцінки їх ефективності.

Глава 4.

КОРОТКИЙ ОГЛЯД СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Методи її захисту від цілеспрямованого доступу:

-обмеження доступу;

-контроль доступу до апаратури, розмежування доступу;

-розділення привілеїв на доступ;

-криптографічне перетворення інформації;

-контроль і облік доступу;

-законодавчі міри.

З появою автоматизованої обробки інформації, збільшенням кількості технічних засобів, що беруть участь в ній, ***збільшується кількість і види випадкових впливів та можливі канали несанкціонованого доступу***.

Глава 4.
КОРОТКИЙ ОГЛЯД СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Із збільшенням імовірності цілеспрямованого несанкціонованого доступу до інформації розвиваються такі ***методи захисту інформації в обчислювальних системах:***

-***методи функціонального контролю***, що забезпечують – ***виявлення і діагностику відмов, збоїв апаратури і помилок*** людини та програмних помилок;

-***методи підвищення достовірності*** інформації;

-***методи захисту інформації від аварійних ситуацій***;

-***методи контролю доступу до внутрішнього монтажу апаратури***, ***ліній зв’язку;***

-***методи розмежування і контролю доступу*** до інформації;

-***методи ідентифікації та аутентифікації користувачів***, технічних засобів, носіїв інформації і документів;

-***методи захисту від побічного випромінювання і наведень.***

Лекція 4
Гарантоздатність автоматизованих систем

Глава 5.
ОБМЕЖЕННЯ ДОСТУПУ

Обмеження доступу полягає в створенні деякої фізичної замкненої перепони навколо об’єкта захисту з організацією контрольованого доступу осіб, пов’язаних з об’єктом захисту за своїми функціональними обов’язками.

Обмеження доступу до комплексів засобів автоматизації обробки інформації полягає:

-у виділенні спеціальної території для розміщення КЗА;

-у спорудженні по периметру зони спеціальних загороджень з охоронною сигналізацією;

-у спорудженні спеціальних будинків ;

-у виділенні спеціальних приміщень в будинку;

-у створенні контрольно-пропускного режиму на території, в будинках і приміщеннях.

Задача засобів обмеження доступу - ***запобігання випадковому і цілеспрямованому доступу сторонніх осіб*** на територію розміщення КЗА і безпосередньо до апаратури.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 5.
ОБМЕЖЕННЯ ДОСТУПУ

З вказаною метою ***створюється захисний контур, що замикається двома видами перепон: фізичною і контрольно-пропускною***. Реалізуються вони як: 1) ***система охоронної сигналізації та 2) система контролю доступу***.

Традиційні засоби контролю доступу в зону, що захищається: виготовлення і видача особам, що допускаються, ***спеціальних перепусток*** з розміщеною на ній фотографією особи власника і відомостей про неї. Дані перепустки можуть зберігатись у власника чи безпосередньо в пропускній кабіні охорони. В останньому випадку допущена особа називає прізвище і свій номер або набирає його на спеціальній панелі кабіни при проходженні через турнікет; пропускне посвідчення випадає з гнізда і попадає в руки працівника охорони, який візуально звіряє особу власника з зображенням на фотографії, назване прізвище з прізвищем на перепустці. Ефективність захисту даної системи вище першої. При цьому виключаються: втрата перепустки, її перехоплення і підробка.

Глава 5.
ОБМЕЖЕННЯ ДОСТУПУ

Для підвищення ефективності захисту з допомогою збільшення кількості параметрів, які перевіряються, використовуються ***біометричні методи*** аутентифікації людини. ***Використовуються ідентифікатори***: відбитки пальців, долоні, голосу, підпису особи, сітківки ока т.і.

Контрольно-пропускні системи реалізуються в напрямку удосконалення конструкції перепустки-посвідчення особи через ***запис кодових значень паролів.***

Фізична перепона захисного контуру, що розміщається по периметру охоронної зони, ***оснащується охоронною сигналізацією.***

Випускаються ***електронні системи для захисту*** державних і приватних об’єктів від проникнення в них сторонніх осіб.

Глава 5.
ОБМЕЖЕННЯ ДОСТУПУ

Ефективність систем охоронної сигналізації визначається: 1) ***типом датчиків, 2) способом оповіщення (контролю), 3) завадостійкістю, 4) реакцією на сигнал тривоги.*** Місцева звукова чи світлова сигналізація може виявитись не достатньою, тому місцеві пристрої охорони доцільно підключати до спеціалізованих засобів централізованого управління, які при отриманні сигналу тривоги висилають спеціальну групу охорони.

Слідкування за станом датчиків здійснює: 1) автоматизована система, розташована в центрі управління, 2) працівник охорони, що знаходиться на об’єкті. В першому випадку місцеві охоронні пристрої підключаються до центру через телефонні лінії, а ***спеціалізований цифровий пристрій здійснює періодичне опитування станів датчиків,*** автоматично набираючи номер приймача-відповідача , розташованого на об’єкті, що охороняється.

Глава 5.
ОБМЕЖЕННЯ ДОСТУПУ

При надходженні в центр сигналу тривоги автоматизована система включає сигнал оповіщення.

Датчики сигналів встановлюються: на різного виду огородженнях, всередині приміщення, безпосередньо на сейфах і т.і.

При розробці комплексної системи охорони конкретного об’єкта враховують його специфіку: внутрішнє планування приміщення, вікон, вхідної двері, розміщення найбільш важливих технічних засобів.

Всі ці фактори впливають на вибір типу датчиків, їх розташування і визначають ряд других особливостей даної системи. ***За принципом дії системи сигналізації можна класифікувати наступним чином***:

- ***традиційні*** з використанням кіл сигналізації та індикації;
-***ультразвукові***;
-***переривання променю***;
-***телевізійні; радіолокаційні; мікрохвильові*** т.і..

Лекція 4
Гарантоздатність автоматизованих систем

Глава 6.
КОНТРОЛЬ ДОСТУПУ ДО АПАРАТУРИ

Для контролю доступу *до внутрішнього монтажу, ліній зв’язку і технологічних органів управління* ***використовується апаратура контролю розкриття апаратури***. Це означає, що внутрішній монтаж апаратури, технологічні органи і пульти управління закриті кришками, дверцятами чи кожухами, на які ***встановлені датчики***. ***Датчики спрацьовують при розкритті апаратури, формують електричні сигнали, які надходять на централізований пристрій збору інформації***. Установлення такої системи має зміст при найбільш повному перекритті усіх технологічних підходів до апаратури, включаючи засоби завантаження програмного забезпечення, пульта управління ЕОМ і зовнішніх кабельних з’єднань технічних засобів, що входять до складу обчислювальної системи.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 6.
КОНТРОЛЬ ДОСТУПУ ДО АПАРАТУРИ

Контроль розкриття апаратури необхідний не тільки в інтересах захисту інформації від НСД, але й ***для дотримання технологічної дисципліни*** з метою забезпечення нормального функціонування обчислювальної системи, тому що часто при експлуатації паралельно рішенню основних задач відбувається ремонт чи профілактика апаратури, і ***може виявитись: 1) випадково забули підключити кабель, 2) з пульта ЕОМ змінили програму обробки інформації.***
З позиції захисту інформації від несанкціонованого доступу ***контроль розкриття апаратури захищає від таких дій:***

-***зміни і руйнування принципової схеми обчислювальної системи*** і апаратури;
-***підключення стороннього пристрою***;
-***зміни алгоритму роботи обчислювальної системи*** шляхом використання технологічних пультів і органів управління;
-***завантаження сторонніх програм*** і внесення ***програмних вірусів*** в систему;
-***використання терміналів сторонніми особами*** і т.і.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 6.
КОНТРОЛЬ ДОСТУПУ ДО АПАРАТУРИ

Основна задача систем контролю розкриття апаратури ***- перекриття на період експлуатації усіх нештатних і технологічних підходів до апаратури***. Якщо останні будуть потрібні в процесі експлуатації системи, апаратура, що вилучається на ремонт чи профілактику, перед початком роботи відключається від робочого контуру обміну інформацією, що підлягає захисту, і вводиться в робочий контур під наглядом і контролем осіб, що відповідають за безпеку інформації. ***Доступ до штатних входів в систему - терміналів*** контролюється ***на рівні видачі механічних ключів користувачам***. ***Доступ до інформації*** контролюється ***за допомогою системи розпізнання і розмежування доступу***, яка включає: ***1) використання кодів паролів, 2) функціональні задачі програмного забезпечення, 3) спеціальний термінал служби безпеки інформації***. Вказаний термінал і пристрій контролю розкриття апаратури входить до складу робочого місця служби безпеки інформації, з якого здійснюється централізований контроль доступу до апаратури, інформації і управління її захистом в даній обчислювальній системі.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 7.
РОЗМЕЖУВАННЯ І КОНТРОЛЬ ДОСТУПУ ДО ІНФОРМАЦІЇ АСОД

Розмежування доступу в обчислювальній системі полягає в ***розділенні інформації, що циркулює в ній, на частини*** і організації доступу до неї посадових осіб у відповідності з їх функціональними обов’язками і повноваженнями.

Задача розмежування доступу: скорочення кількості посадових осіб, що не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед допущеного до роботи персоналу.

При цьому ***поділ інформації може проводитись*** за: 1) ***ступенем важливості, 2) функціональним призначенням, 3) документами*** і т.і.

Оскільки ***доступ здійснюється з різних технічних засобів***, то ***першим є розмежування доступу до технічних засобів*** шляхом розміщення їх в окремих приміщеннях. Усі функції підготовки технічного обслуговування апаратури, її ремонту, профілактики, перезавантаження програмного забезпечення повинні бути технічно і організаційно відділені від основних задач системи. КЗА і організація, що його обслуговує повинні бути побудовані таким чином:

Глава 7.
РОЗМЕЖУВАННЯ І КОНТРОЛЬ ДОСТУПУ ДО ІНФОРМАЦІЇ АСОД

-технічне обслуговування КЗА в процесі експлуатації повинно виконуватись окремим персоналом без доступу до інформації, що підлягає захисту;

-перезавантаження програмного забезпечення і всякі його зміни повинні - проводитись спеціально виділеним для цієї мети перевіреним спеціалістом;

-функції забезпечення безпеки інформації повинні виконуватись спеціальним - підрозділом в організації - власника КЗА, обчислювальної мережі чи АСУ;

-організація доступу користувачів до пам’яті КЗА повинна забезпечувати можливість розмежування доступу до інформації, що зберігається в ній, з достатнім ступенем деталізації і у відповідності з заданими рівнями повноважень користувачів;

-реєстрація і документування технологічної і оперативної інформації повинні бути розділені.

Розмежування доступу користувачів - споживачів КЗА здійснюється за такими параметрами:

-за виглядом, характером, призначенням, ступенем важливості та секретності інформації;

Глава 7.
РОЗМЕЖУВАННЯ І КОНТРОЛЬ ДОСТУПУ ДО ІНФОРМАЦІЇ АСОД

- ***за способом її обробки***: зчитуванням, записом, внесенням змін, виконанням команд;
- ***за умовним номером терміналу;***
- ***за часом обробки***.

Принципова можливість розмежування за вказаним параметром повинна бути забезпечена проектом КЗА. Конкретне розмежування при експлуатації КЗА установлюється споживачем і вводиться в систему його підрозділом, що відповідає за безпеку інформації.

При проектуванні обчислювального комплексу для побудови КЗА використовуються:

- розробка операційної системи з можливістю реалізації розмежування доступу до інформації, що зберігається в пам’яті ОК;
- ізоляція областей доступу;
- розділення бази даних на групи;
- процедури контролю перелічених функцій.

Глава 7.
РОЗМЕЖУВАННЯ І КОНТРОЛЬ ДОСТУПУ ДО ІНФОРМАЦІЇ АСОД

При проектуванні КЗА та інформаційної системи АСУ (мережі) на їх базі проводяться:

- розробка і реалізація функціональних задач по розмежуванню і контролю доступу до апаратури і інформації як в рамках даного КЗА, так і АСУ (мережі) в цілому;
- розробка апаратних засобів ідентифікації і аутентифікації користувача;
- розробка програмних засобів контролю і управління розмежуванням доступу;
- розробка окремої експлуатаційної документації на засоби ідентифікації, аутентифікації, розмежуванню і контролю доступу.

В якості ідентифікаторів особи для реалізації розмежування на практиці використовуються коди паролів, які зберігаються в пам’яті користувача КЗА. Для допомоги користувачу в системах з підвищеними вимогами ***великі значення кодів паролів записуються на спеціальні носії - електронні ключі чи картки.***

Лекція 4
Гарантоздатність автоматизованих систем

Глава 8.
РОЗДІЛЕННЯ ПРИВІЛЕЇВ НА ДОСТУП

Розділення привілеїв на доступ до інформації: з числа допущених до неї посадових осіб виділяється група, якій надається доступ тільки при одночасному пред’явленні повноважень усіх членів групи.

Задача вказаного методу - істотно утруднити цілеспрямоване перехоплення інформації порушником. ***Приклад такого доступу – 1) сейф з декількома ключами, замок якого відкривається тільки при наявності усіх ключів.*** Аналогічно в АСОД може бути передбачений ***2) механізм розділення привілеїв при доступі до особливо важливих даних з допомогою кодів паролів.***

Даний метод дещо ускладнює процедуру, але має захист високої ефективності. ***Поєднання подвійного криптографічного перетворення інформації і методу розділення привілеїв*** дозволяє забезпечити високоефективний захист інформації від цілеспрямованого НСД.

Глава 8.
РОЗДІЛЕННЯ ПРИВІЛЕЇВ НА ДОСТУП

Крім того, при наявності дефіциту в засобах, а також з метою постійного контролю доступу до цінної інформації зі сторони адміністрації користувача АСУ в деяких випадках можливий варіант використання права на доступ до інформації нижче стоячого керівника тільки при наявності його ідентифікатора та ідентифікатора його замісника чи представника служби безпеки інформації. При цьому інформація видається на дисплей тільки керівника, а на дисплей підлеглого - тільки інформація за фактом її запиту.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА (СУБ’ЄКТА)

9.1. Об’єкт ідентифікації і встановлення відповідності: узагальнення

Ідентифікація - це присвоєння якому-небудь об’єкту чи суб’єкту унікального образу, імені, числа. ***Встановлення відповідності*** (**аутентифікація**) полягає в перевірці, чи є об’єкт (суб’єкт), що перевіряється саме тим, за кого себе видає. ***Кінцева мета ідентифікації і встановлення відповідності об’єкта в обчислювальній системі*** – **допуск** до інформації обмеженого користування у випадку позитивної відповіді; **відмова** в допуску у випадку негативної відповіді при перевірці. ***Об’єктами ідентифікації і встановлення відповідності в обчислювальній системі є***:

1) людина (оператор, користувач, посадова особа);
2) технічний засіб (термінал, дисплей, ЕОМ, КСА);
3) документи;
4) носії інформації (магнітні стрічки, диски і інші);
5) інформація на дисплеї, табло т.і.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

Встановлення відповідності об’єкта може проводитись: людиною, апаратним засобом, програмою, обчислювальною системою.

В обчислювальних системах використання вказаних методів з метою захисту інформації при її обміні передбачає конфіденційність образів і імен об’єктів.

При обміні інформацією між людиною і ЕОМ, обчислювальними системами в мережі рекомендується передбачити взаємну перевірку відповідності повноважень об’єкта чи суб’єкта. З вказаною метою необхідно, щоб кожен з об’єктів (суб’єктів) зберігав в своїй пам’яті, недоступній для сторонніх, список образів (імен) об’єктів (суб’єктів), з яким проводиться обмін інформацією, що підлягає захисту.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

9.2. Ідентифікація і встановлення відповідності – 1) особи

Ідентифікатором особи є: форма голови, риси обличчя, характер, її звички, поведінка та інші ознаки, які створюють образ людини, який ми зберігаємо у своїй пам’яті. При появі людини за цими ознаками ми впізнаємо чи не впізнаємо в ній свого знайомого. З плином часу після тривалої перерви поступово ті чи інші ознаки стираються з нашої пам’яті. З плином часу змінюється також сама людина - об’єкт ідентифікації.

Відомо, що ***відбитки пальців і обриси долоні руки, тембр голосу, особовий підпис та інші елементи особистості*** носять індивідуальний характер і зберігаються на протязі всього життя людини.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

Для виконання процедури встановлення відповідності необхідно щоб образ, що знімається з особистості користувача, збігався з образом, що зберігається в пам’яті обчислювальної системи. У випадку відмови у доступі система повинна мати властивість відрізняти подібні образи. Тут існує дві задачі, які необхідно вирішити одночасно.

Для виконання допуску - не вимагається великого об’єму інформації про образ (можна сказати навіть, що чим менше, тим краще). А ***для виконання відмови*** - інформацію про образ необхідно збільшити на максимально можливу величину.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

Із збільшенням об’єму інформації про образ з метою точної перевірки особистості і найбільшої кількості її параметрів збільшується імовірність їх зміни в часі та незбігання з параметрами образу, що зберігається системою перевірки, ростуть об’єми пам’яті, ускладнюється апаратура і, отже, збільшується імовірність відмов в доступі особі, що має на це право.

Відправною точкою при розробці систем розпізнавання образів є підвищення точності відтворення образу з метою автоматичного відбору з множини потенційних образів єдиного, що зберігається в пам’яті машини.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА (СУБ’ЄКТА)

Запитання: 1) ***Яка повинна бути точність відтворення образу ?*** **2)** ***Яка повинна бути різниця між образом особи, якій дозволений доступ, і образом потенційного порушника?*** **3)** ***Яка імовірність появи порушника, образ якого наближується до образу, що зберігається в пам’яті обчислювальної системи?*** На ці питання відповіді немає.

Роботи по системам розпізнавання образів з метою широкого використання для захисту інформації в обчислювальних системах - недоцільні. Крім того, системи ідентифікації і встановлення відповідності особи, основані на антропометричних і фізіологічних даних людини, ***не відповідають найбільш важливій вимозі: конфіденційності,*** оскільки записані на фізичні носії дані зберігаються постійно і фактично є ключем до інформації, що повинна захищатися, а постійний ключ в кінці кінців стає доступним.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

1) ***Розповсюдженою і простою системою аутентифікації є*** - ***ключ-замок***, в якій власник ключа є об’єктом встановлення відповідності. Але ключ можна загубити, викрасти і зняти з нього копію, так як ідентифікатор особи фізично від неї відділений. Система ключ-замок має локальне використання. В електромеханічному замку замість ключа може використовуватись код.

2) ***Розповсюдженим методом аутентифікації є*** - ***присвоєння собі чи іншому об’єкту унікального імені чи числа - пароля*** і зберігання його значення в обчислювальній системі. ***При вході в обчислювальну систему користувач вводить через термінал свій код пароля***, обчислювальна система порівнює його значення із значенням, що зберігається в пам’яті, і при збіганні кодів відкриває доступ до дозволеної функціональної задачі, а при незбіганні - відмовляє в ньому. Приклад процедури ідентифікації і установлення відповідності користувача наведений на рис. 9.1.

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА (СУБ’ЄКТА)

3) ***Найбільш високий рівень безпеки входу в систему досягається розділенням коду пароля на дві частини:*** **одна** ***запам’ятовується користувачем і вводиться вручну;*** **друга** ***- розміщується на спеціальному пристрої зчитування, що зв’язане з терміналом.*** В цьому випадку ідентифікатор зв’язаний з особистістю користувача, розмір пароля може легко запам’ятовується, і при викраденні картки у користувача буде час для заміни коду і одержання нової картки.

На випадок захисту частини паролю, що запам’ятовується, від отримання її порушником шляхом фізичного примушення користувача, можливо, буде корисно в обчислювальній системі передбачити механізм тривожної сигналізації, який реалізується на використанні фальшивого паролю. Фальшивий пароль запам’ятовується користувачем одночасно із справжнім і повідомляється зловмиснику.

Національний університет “Львівська політехніка”
Кафедра захисту інформації
Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’

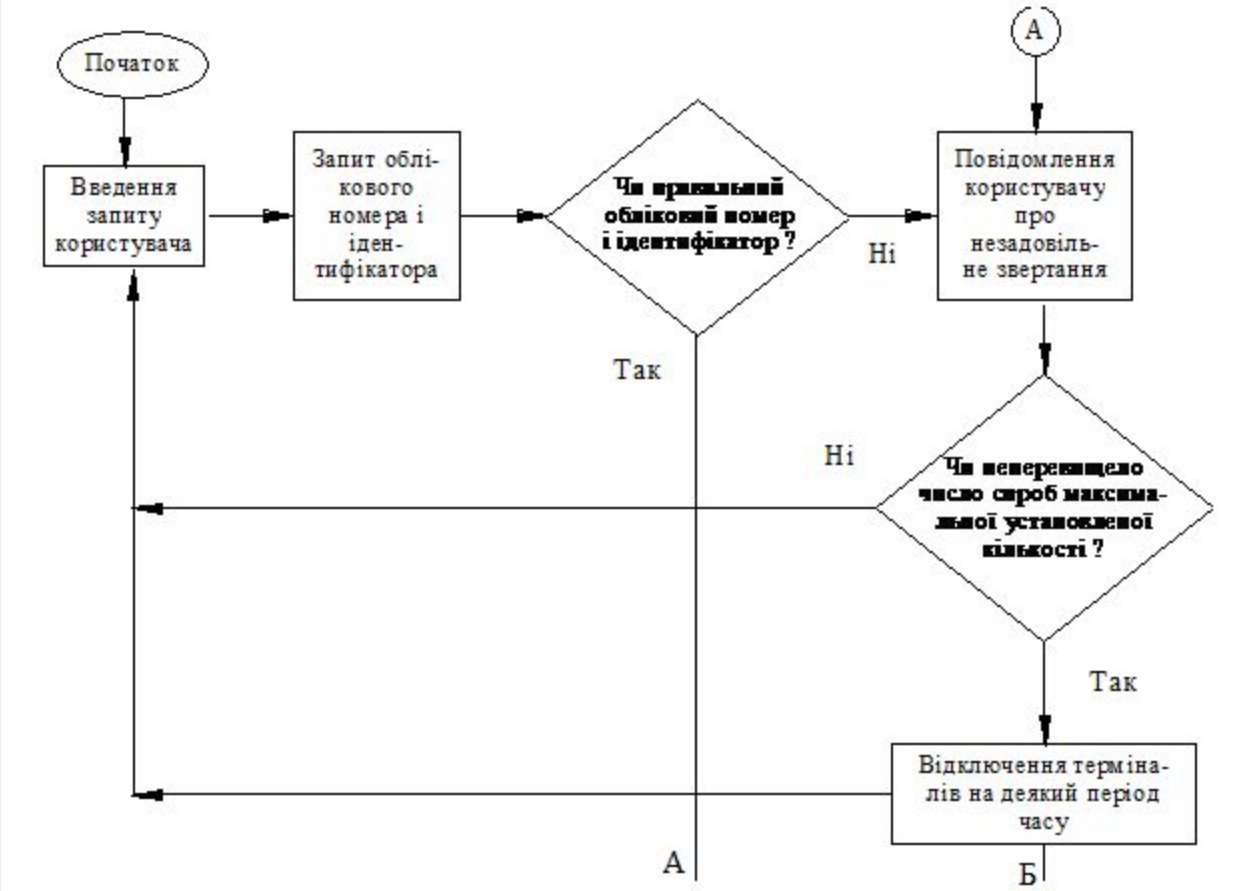


Рис 9.1 Ідентифікація та встановлення відповідності

Лекція 4
Гарантоздатність автоматизованих систем

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

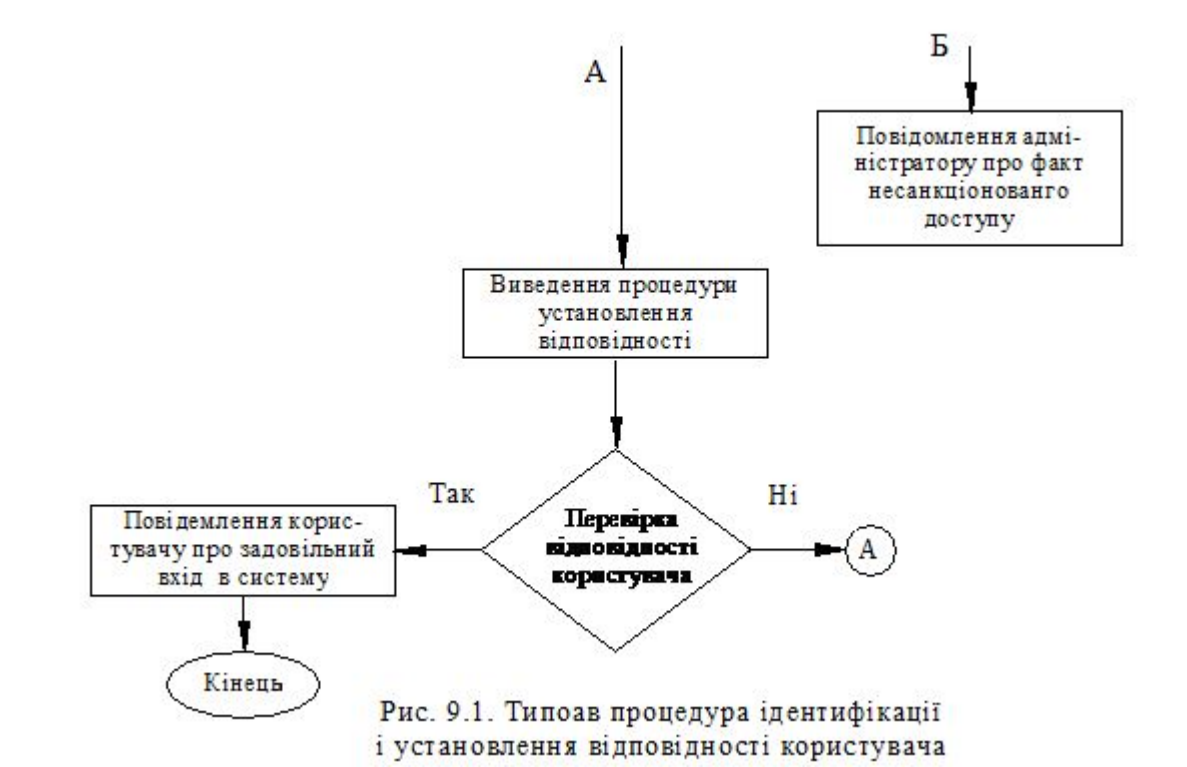


Рис. 9.1. Типоав процедура ідентифікації і установлення відповідності користувача

Рис.9.1продовження

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

Необхідно в обчислювальній системі одночасно з прихованою сигналізацією передбачити механізм обов’язкового виконання вимог зловмисника, що скористався засобами аутентифікації законного користувача. ***Окрім методів паролів в обчислювальних системах в якості засобів аутентифікації використовують методи запит-відповідь і рукостискання.***

В методі запит-відповідь набір відповідей на т стандартних, орієнтованих на користувача питань зберігається в ЕОМ і управляється операційною системою. Коли користувач робить спробу включитись в роботу, операційна система випадковим чином вибирає і задає йому деякі (чи всі) з цих питань. ***Правильні відповіді користувача на вказані питання відкривають доступ до системи.***

Для усунення деяких недоліків описаних вище методів операційна система може вимагати, щоб користувач зміг довести свою відповідність з допомогою конкретної обробки алгоритмів. Цю частину називають процедурою в режимі рукостискання, вона може бути виконана як між двома ЕОМ, так і між користувачем і ЕОМ.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКА)

9.3. Ідентифікація і встановлення відповідності – 2) технічних засобів

При організації системи захисту інформації в обчислювальні системі актуальною є - ***ідентифікація і встановлення відповідності терміналу, з якого заходить в систему користувач.***

Процедура може здійснюватись за допомогою паролів. ***Пароль можна використати*** не тільки для аутентифікації користувача і терміналу по відношенню до системи, але й ***для зворотного установлення відповідності ЕОМ по відношенню до користувача.***

.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

9.4. Ідентифікація і встановлення відповідності – 3) документів

В обчислювальних системах в якості документів, що є продуктами інформаційної системи є: *1) інформація роздрукована на принтерах; 2) магнітні диски 3) інші постійні запам’ятовуючі пристрої довготривалого зберігання у вигляді фізичних носіїв.*

Необхідно відповідність документа розглядати з двох позицій:

1) одержання документа, сформованого безпосередньо даною системою та на обладнанні її документування;

2) одержання готового документа з віддалених об’єктів обчислювальної мережі чи АСУ.

В першому випадку відповідність документа гарантується обчислювальною системою, що має засоби захисту інформації від НСД, а також фізичними характеристиками принтерів, що притаманні тільки даному пристрою.

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

Ефективним засобом є - використання криптографічного перетворення інформації . ***Інформація, що закрита кодом пароля***, відомим тільки особі, що її передає і одержувачу, не викликає сумніву в її відповідності. Якщо код пароля, що використовується в даному випадку, використовується тільки особою, що передає, і вводиться нею особисто, можна стверджувати, що пароль є її особистим підписом.

Криптографічне перетворення інформації для ідентифікації і встановлення відповідності документа в другому випадку, коли документ транспортувався по території, що не охороняється, з територіально віддаленого об’єкта чи тривалий час знаходився на зберіганні, також є найбільш ефективним засобом. Однак при відсутності необхідного для цієї мети обладнання невисокі вимоги до захисту інформації інколи дозволяють використовувати більш прості засоби ідентифікації і встановлення відповідності документів: опечатування і опломбування носіїв документів із забезпеченням їх охорони.

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

При неавтоматизованому обміні інформацією - відповідність документа посвічується особистим підписом людини, автора (авторів) документа. Перевірка відповідності документа в цьому випадку звичайно полягає у візуальній перевірці збігання зображення підпису на документі із зразком оригіналу. При цьому підпис розташовується на одному листі разом з текстом чи частиною тексту документа, підтверджуючи тим самим відповідність тексту. При криміналістичній експертизі перевіряються ще інші параметри відповідності документа.

При автоматизованій передачі документів каналами зв’язку (які розташовані на неконтрольованій території) - змінюються умови передачі документа. В цих умовах навіть якщо зробити апаратуру, що сприймає і передає зображення підпису автора документа, його одержувач отримає не оригінал, а лише копію підпису, який в процесі передачі може бути повторно копійований для використання при передачі фальшивого документа.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

При передачі документів по каналах зв’язку в обчислювальній мережі використовується криптографічне перетворення інформації.

Сфера використання цифрового підпису надзвичайно широка: від проведення фінансових і банківських операцій до контролю за виконанням міжнародних угод і охорони авторських прав. Учасники обміну документами потребують захисту від таких цілеспрямованих несанкціонований дій:

- відмови відправника від переданого повідомлення;
- фальсифікації (підробки) одержувачем отриманого повідомлення;
- зміна одержувачем отриманого повідомлення;
- маскування відправника під іншого абонента.

Забезпечення захисту кожної сторони, що бере участь в обміні, здійснюється за допомогою введення спеціальних протоколів. Для верифікації повідомлень протокол повинен містити обов’язкові положення:

Лекція 4
Гарантоздатність автоматизованих систем

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКА)

1) одержувач повідомлення повинен мати можливість впевнитись, що отриманий в складі повідомлення підпис є правильним підписом відправника;
2) отримання правильного підпису відправника можливе тільки при використанні закритої інформації, якою володіє тільки відправник;
3) для виключення можливості повторного використання застарілих повідомлень верифікація повинна залежати від часу.

Підпис повідомлення є способом шифрування повідомлення з допомогою криптографічного перетворення. Елементом, що закривається, в повідомленні є код ключа. Якщо ключ підпису належить скінченій множині ключів, якщо ця множина достатньо велика, а ключ підпису визначається методом випадкового вибору, то повна перевірка ключів підпису для пар повідомлення - одержувач з обчислювальної точки зору еквівалентна пошуку ключа. ***Підпис є паролем, що залежить від відправника, одержувача і змісту повідомлення, що передається.*** Підпис повинен змінюватись від повідомлення до повідомлення.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 9.
ІДЕНТИФІКАЦІЯ І ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОБ’ЄКТА(СУБ’ЄКТА)

9.5. Ідентифікація і встановлення відповідності – 4) інформації на засобах її відображення і друку

В системах з централізованою обробкою інформації *встановлення її відповідності на технічних засобах відображення і друку* ***гарантується наявністю системи захисту інформації даної обчислювальної системи.*** В більш відповідальних випадках окремі повідомлення чи блоки інформації підлягають *спеціальному захисту, який полягає в створенні засобів підвищення достовірності інформації і криптографічного перетворення*. Установлення відповідності отриманої інформації, включаючи відображення на табло і терміналах, полягає в контролі результатів забезпечення достовірності інформації і результатів дешифрування отриманої інформації до відображення її на екрані.

Глава 10.
ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВЕДЕНЬ

10.1. Потенційні загрози

Робота засобів обчислювальної техніки супроводжується електромагнітним випромінюваннями і наводками на з’єднувальні провідні лінії, кола живлення, земля, що виникають внаслідок електромагнітних взаємодій в ближній зоні випромінювання, в яку можуть потрапити також провідники допоміжньої і сторонньої апаратури. ***Електромагнітні випромінювання, навіть якщо вони відповідають допустимим технічним нормам, є небезпечними з точки зору витоку секретної інформації і несанкціонованого доступу до неї.***

Інформацію, що обробляється засобами електронно-обчислювальної техніки (ЕОТ), ***можна відновити шляхом аналізу електромагнітних випромінювань і наведень. Для цього необхідні їх прийом і декодування***. Певний час вважалось дуже важкою справою розшифрувати інформацію, що міститься в випромінюванні, і що тому відновлення інформації після прийому під силу тільки фахівцям, що мають у розпорядженні дуже складну апаратуру виявлення і декодування.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 10.
ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВОДОК

Відновлення інформації від деяких засобів ЕОТ можливе з допомогою загальнодоступних радіоелектронних засобів. При відновленні інформації з дисплеїв можна використати звичайний чорно-білий телевізор. Якщо дисплей є елементом обчислювальної системи, то він може виявитись найбільш слабкою її ланкою, яка знецінить усі міри по збільшенню безпеки випромінювань, що прийняті у всіх інших частинах системи.

Використання в засобах ЕОТ імпульсних сигналів прямокутної форми і високочастотної комутації призводить до того, що в спектрі випромінювань будуть компоненти з частотами аж до НВЧ. Хоча енергетичний спектр сигналів зменшується з ростом частоти, але ефективність випромінювання при цьому збільшується, і рівень випромінювань може залишатись постійним до частот в декілька ГГц. Резонанси, що виникають через паразитні зв’язки, можуть викликати підсилення випромінювання сигналів на деяких частотах спектру.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 10.
ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВЕДЕНЬ

10.2. Методи і засоби захисту інформації від побічного електромагнітного випромінювання і наведень інформації

З метою захисту секретної інформації від витоку за рахунок побічного електромагнітного випромінювання і наведень виконується вимірювання рівня небезпечних сигналів на відстані від джерела (дисплея, принтера, кабелю). Заміри виконуються в декількох точках на різних відстанях від джерела з допомогою спеціальної приймальної апаратури (аналізатора спектру НТР 8585 А в діапазоні 30 ... 100 МГц в режимі із смугою пропускання 10 кГц і піковим детектуванням). ***Якщо рівень сигналу на межі установленої зони перевищив допустиме значення, використовують захисні міри. Захисні міри:*** 1) удосконалення апаратури з метою зменшення рівня сигналів, 2) установлення спеціальних фільтрів, генераторів шуму, які працюють паралельно, 3) спеціальних екранів т.і.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 10.
ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВОДОК

До захисних мір відноситься використання в лініях і каналах зв’язку волоконно-оптичних кабелів, які мають переваги: 1) відсутність електромагнітного випромінювання у зовнішнє середовище, 2) стійкість до зовнішнього електромагнітного середовища, 3) велику завадостійкість, 4) скритність передачі, 5) малі габарити (що дозволяє прокладати їх поруч з вже існуючими кабельними лініями), стійкість до впливів агресивного середовища.

З точки зору захисту інформації волоконно-оптичні кабелі мають ще одну перевагу: підключення до них з метою перехоплення даних, що передаються, є значно більш складною задачею, ніж підключення до звичайного провідника чи кабелю з допомогою індуктивних датчиків і прямого підключення. ***Використання електрооптичних і оптоелектричних перетворювачів забезпечують безпеку інформації.***

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 10.
ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВЕДЕНЬ

Метод передачі даних між різними пристроями в межах одного обчислювального центру з використанням інфрачервоних (ІЧ) систем має перевагою те, що ІЧ-канали передачі даних не чутливі до електромагнітних випромінювань обладнання, що працює в цьому ж приміщенні. Спеціалісти вважають, що використання цієї системи повністю усуває можливість проникнення електромагнітного випромінювання за межі обчислювального центру.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Використовуються: ***1) для захисту функціонування*** АСОД від випадкових впливів - ***засоби підвищення надійності*** *апаратури і програмного забезпечення КЗА;* ***2) для захисту інформації - засоби підвищення її достовірності; 3) для запобігання аварійних ситуацій - використовуються спеціальні міри.***

Методи і засоби підвищення надійності обчислювальних систем і достовірності інформації в теперішній час достатньо добре розроблені, і по цим питанням є достатньо апаратури. Перші методи і засоби опосередкованим чином допомагають істотно зменшити вплив випадкових впливів і на інформацію.

Ми зупинимось лише на введенні в проблему і основних її моментах, що мають безпосереднє відношення до захисту інформації в рамках поставленої задачі і необхідних для аналізу і вироблення нового підходу до засобів підвищення надійності з позиції безпеки інформації, що опрацьовується в АСОД.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Проблема надійності автоматизованих систем вирішується трьома шляхами: 1) підвищенням надійності деталей і вузлів; 2) побудовою надійних систем з менш надійних елементів за рахунок структурної надлишковості (дублювання елементів, пристроїв, підсистем і т.п.); 2) використанням функціонального контролю (ФК)з діагностикою відмов, який збільшує надійність функціонування системи шляхом скорочення часу відновлення апаратури, що відмовила.

Задачами функціонального контролю системи є: *1) своєчасне виявлення збоїв*, несправностей і програмних помилок; *2) виключення їх впливу на подальший процес обробки інформації; 3) виявлення місця елементу, що відмовив, чи блоку програми з метою наступного швидкого відновлення системи.*

Існуючі методи функціонального контролю обчислювальних систем поділяються на: 1) програмні, 2) апаратні і комбіновані (поєднання програмних з апаратними).

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Порівняльна характеристика методів ФК враховує наступні фактори:

-1) *надійність виявлення*;

- 2) *можливість виправлення помилок після збоїв* без втручання оператора;

- 3) *час, що витрачається на усунення випадкових помилок*;

- 4) *кількість додаткового обладнання;*

- 5) *способи використання*: паралельно; перериванням обробки інформації;

- 6) *вплив контролю на швидкодію* обчислювальної системи чи її продуктивність;

- 7) *зазначення місця несправності* з необхідною точністю.

Програмний контроль поділяється на: 1) програмно-логічний, 2) алгоритмічний, 3) тестовий.

Програмно-логічний контроль - це подвійний рахунок з порівнянням отриманих результатів. ***Алгоритмічний контроль*** - задача, що вирішена за певним алгоритмом, перевіряється повторно за скороченим алгоритмом з достатнім ступенем точності.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

ОСОБЛИВОСТІ: **1)** ***Програмно-логічний контроль дозволяє надійно виявляти збої, і для його реалізації не потрібно додаткового обладнання***. Але при ньому більше, ніж вдвоє зменшується продуктивність ЕОМ, не виявляються систематичні збої, неможливо виявити місце відмови і тим більше збою, необхідна додаткова ємність пам’яті для програми обчислень. 2) ***При алгоритмічному контролі продуктивність ЕОМ вища***; має обмежене використання, оскільки не завжди вдається знайти для основного алгоритму скорочений, який був би значно коротший від основного.

Тестовий контроль - ***використовується для перевірки роботоздатності комплексу засобів автоматизації за допомогою випробовувальних програм.***

3) Тестовий контроль на відміну від програмно-логічного перевіряє не процес переробки інформації, а перебування КЗА чи його частини в роботоздатному стані. Крім того, тестовий контроль не завжди виявляє збої і під час перевірки не може вирішувати задачі за робочою програмою.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Широке використання знаходять методи: 1) апаратного схемного контролю; 2) комбінований метод.

Апаратний контроль на відміну від програмного може забезпечити вказівку про наявність збою чи несправності безпосередньо в момент їх виникнення.

Апаратний контроль в КЗА поділяється на: *1) контроль за модулем; 2) контроль при дублюванні обладнання; 3) контроль при потроєнні обладнання* з використанням мажоритарних елементів.

1) Контроль за модулем: з теорії чисел відомо, що ціле додатне число можна представити у вигляді порівняння:

$$A = r_a \pmod{M} \qquad (1)$$

яке установлює наступні співвідношення між числами A, r_a і M:

$$A = Ml + r_a$$

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

де A, M, l і r_a - цілі числа; A - будь-яке n-розрядне число, що контролюється; M - модуль (дільник); l - частка; r_a - залишок від ділення A на модуль M (контрольний код числа A).

При даному методі контролю кожному члену, що контролюється, додається ще m додаткових розрядів, в яких записується контрольний код, тобто залишок r_a. Якщо записати всі числа у вигляді порівняння (12.1), то після цього їх можна буде додавати, множити, а результат записувати у вигляді подібних порівнянь:

$$\sum_{i=1}^{p} A_i = \sum_{i=1}^{p} r_{a_i} (\mathrm{mod}\, M) \qquad (12.2)$$

$$\prod_{i=1}^{p} A_i = \prod_{i=1}^{p} r_{a_i} (\mathrm{mod}\, M) \qquad (12.3)$$

Вирази (12.2) і (12.3) означають, що сума (добуток) чисел є порівняною з сумою (добутком) залишків цих чисел за модулем M. Технічна реалізація контролю за модулем - розроблення спеціальних схем (згорток). Ефективність контролю збільшується із збільшенням модуля.

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Однак із збільшенням М не пропорційно збільшується кількість додаткового обладнання і ускладнюється схема контролю. *Широке розповсюдження в обчислювальних схемах отримав контроль за модулем 2.*

2) Дублювання обладнання - ***дозволяє шляхом порівняння вихідних сигналів виявити відмову апаратури.*** Висока ефективність такого контролю базується на тому, що імовірність одночасної відмови двох однакових елементів дуже мала. Недоліком цього методу є те, що не завжди є можливість виявити, який з каналів є справним, і тому, щоб процес функціонування залишався справним, доводиться одночасно в кожному з каналів використовувати методи контролю, наприклад контроль за модулем.

3) Потроєння обладнання - ***дозволяє поряд із збільшенням імовірності безвідмовної роботи збільшити і достовірність функціонування за допомогою мажоритарних елементів.*** Даний метод потребує, зрозуміло, збільшення об’ємів обладнання.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Оскільки результат впливу на інформацію залежить від кількості помилок в даний момент часу, розглянемо імовірність появи цих подій.

Введення, зберігання і обробка інформації в КЗА здійснюється за допомогою кодів чисел і слів за певним алгоритмом. Поява збоїв призводить до того, що в коді може виникнути однократна чи групова помилка (двократна, трикратна і т.д.). Помилка однократна, *якщо вона виникла в одному розряді коду числа чи слова .*

Вважаючи помилки в кожному розряді коду незалежними, можна визначити імовірність виникнення помилки *i*-ї кратності при відомій імовірності спотворення одного розряду двійкового коду. В цьому випадку помилки в кожному з розрядів підпадають під біномний розподіл імовірностей. ***Імовірність появи однократної помилки*** *в n-розрядному двійковому коді* може бути визначена з виразу

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

$$P_i = nq\ \ (1-q)^{n-1}$$

де q - імовірність появи помилки в окремому розряді на протязі одної операції.

***Імовірність появи двократної помилки*:**

$$P_2 = \frac{n\,(n-1)}{2} q^2 (1-q)^{n-2}$$

***Імовірність появи помилки і-ої кратності*:**

$$P_i = C_n^i q^i (1-q)^{n-i}$$

Оцінка значення P_i аналітичним шляхом пов’язана із складностями, що залежать від причин, які спричиняють збої. Тому, P_i може бути отримано з допомогою більш зручної формули

$$P_i = \frac{n\mu_p t_{on}}{i!} e^{-n\mu_p t_{on}}$$

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

де t_{on} - тривалість однієї операції; - інтенсивність відмов обладнання, що бере участь в передачі і зберіганні кожного розряду двійкового коду.

Із збільшенням кратності помилки імовірність її появи зменшується. Імовірність появи помилки з кратністю i=4 настільки мала, що нею можна знехтувати. ***Для оцінки ефективності апаратного контролю необхідно знати імовірність виявлення (пропуску) помилок різної кратності при вибраному методі контролю.*** **В зв’язку з цим загальна імовірність пропуску помилки**

$$P_{пр} = \sum_{i=1}^{n} P_i \; P_{mпрi}$$

де P_i - імовірність виникнення помилки і-ої кратності; $P_{м.пр.i}$ - імовірність пропуску помилки і-ої кратності при вибраному методі апаратного контролю.

А) Імовірність появи двократної помилки можна вирахувати за формулою

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

$$P_2 = \frac{n^2 \mu_p^2 t_{on}^2}{2} e^{-n\mu t_{on}}$$

В) Імовірність пропуску двократної помилки* при контролі за модулем 3 *вираховується за формулою

$$P_{np} = 0.25 n^2 \mu_p^2 t_{on}^2 (1 + 0.166\ n\mu_p t_{on})$$

Здатність засобів ФК своєчасно забезпечувати виявлення і блокування помилок заданої кратності визначає* рівень достовірності контролю обробки інформації.** Для якості ФК відіграє щільність розподілу його засобів виявлення помилок по всій □площі□ контрольованої обчислювальної системи, тобто повнота її охоплення функціональним контролем. ***При створенні обчислювальних систем використовуються наступні показники якості ФК:

1) **час виявлення і локалізації відмов апаратури** з точністю до елемента, що знімається:

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

$$T_{вияв} = \frac{\sum_{i=1}^{m} t_{\text{вияв}_i}}{m}$$

де m - число експериментів; i - номер експерименту; $t_{вияві}$ - час виявлення відмови в і-му експерименті;

2) **повнота контролю функціонування обчислювальної системи:**

$$K_n = \frac{\lambda_k}{\lambda_o}$$

де λ_k - сумарна інтенсивність появи відмов складових частин, охоплених контролем; λ_o - сумарна інтенсивність відмов всіх складових частин обчислювальної системи;

3) **достовірність контролю**:

$$K_Д = \frac{m_{вияв}}{n_{пр}}$$

де $m_{вияв}$ - загальна кількість відмов, що виявлені даною системою функціонального контролю; $n_{пр}$- загальна кількість відмов проведення ФК при умові появи чи штучного введення відмов в кожному досліді.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Ефективне функціонування автоматизованої системи - забезпечення необхідного рівня достовірності інформації. ***Достовірність інформації в системі*: реальна інформація в системі про деякий параметр не збігається в межах заданої точності з істинним значенням.**

Необхідна достовірність досягається використанням різних методів, реалізація яких вимагає ***внесення в системи обробки даних інформаційної, часової чи структурної надлишковості.*** **Достовірність при обробці даних досягається** шляхом: 1) контролю і виявлення помилок в початкових і результуючих даних, 2) їх локалізації; 3) виправлення. ***Умови підвищення достовірності*** - зменшення частки помилок до припустимого рівня.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Методи контролю **при обробці інформації** *в системі класифікуються за різними параметрами:* 1) ***за кількістю операцій,*** що охоплюються контролем, - **одиничний** (одна операція), **груповий** (група послідовних операцій), **комплексний** (контролюється, наприклад, процес збору даних); 2) ***за частотою контролю*** **- безперервний, циклічний, періодичний, разовий, вибірковий, за відхиленням**; 3) ***за часом контролю*** **- до виконання основних операцій; одночасно з ними; в проміжках між основними операціями; після них**; 4) ***за видом обладнання контролю*** – **вбудований; контроль з допомогою додаткових технічних засобів; безапаратний;** 5) ***за рівнем автоматизації***: **ручний, автоматизований, автоматичний**.

Системні, програмні і апаратні методи контролю достовірності.

1. Системні методи включають: 1) оптимізацію структури обробки; 2) підтримку характеристик обладнання в заданих межах; 3) визначення оптимальної величини пакетів даних і швидкості початкової обробки т.і.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

2. ***Програмні методи підвищення достовірності інформації:*** при складанні процедур обробки даних в них передбачають додаткові операції, що мають математичний чи логічний зв’язок з алгоритмом обробки даних. Порівняння результатів цих додаткових операцій з результатами обробки даних дозволяє виявити з певною імовірністю наявність чи відсутність помилок.

3. Апаратні методи контролю і виявлення помилок можуть виконувати практично ті ж самі функції, що й програмні. Апаратними методами виявляють помилки скоріше і ближче до місця їх виникнення, а також помилки, що є недоступні для програмних методів.

Ці методи обробки даних базуються на використанні певної надлишковості. Розрізняють методи контролю *із: 1) структурною, 2) часовою, 3) інформаційною надлишковістю.*

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Структурна надлишковість вимагає введення в склад системи додаткових елементів (резервування інформаційних масивів і програмних модулів, реалізації одних і тих самих функцій різними програмами).

Часова надлишковість пов’язана з можливістю неодноразового повторення певного контрольованого етапу обробки даних. Звичайно етап обробки повторюють неодноразово і результати обробки порівнюють між собою. У випадку виявлення помилки проводять виправлення і повторну обробку.

Інформаційна надлишковість: ***природна і штучна***. Природна інформаційна надлишковість віддзеркалює ***існуючі зв’язки між елементами обробки***, наявність яких дозволяє робити висновки про достовірність інформації. ***Штучна інформаційна надлишковість полягає у введенні***: 1) додаткових інформаційних розрядів в цифровому представленні даних, що обробляються; 2) додаткових операцій в процедурі їх обробки.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

На основі аналізу результатів: додаткових операцій, процедур обробки даних, додаткових інформаційних розрядів виявляється наявність чи відсутність помилок певного типу, а також можливість їх виправлення.

В роботах по підвищенню достовірності інформації розглядаються разом ***завадостійкість і надійність систем передачі і обробки інформації*** з позиції якості таких систем. В залежності від характеру інформації, особливостей алгоритму системи, а також від задач, що стоять перед її адресатами, визначають **залежність змісту інформації від помилок при її передачі**:

1) змістовний об’єм інформації в повідомленні зменшується пропорційно числу спотворень розрядів в кодовій комбінації повідомлення;

2) спотворення одного чи декількох розрядів призводить майже до повної втрати решти інформації. Розглянемо засоби ФК і підвищення достовірності інформації у контексті захисту ***від: 1) випадкових руйнувань, 2) модифікації, 3) витоку інформації.***

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Відмови, збої в апаратурі і помилки в програмному забезпеченні можуть призвести до порушення функціонування обчислювальної системи, до руйнування і зміни інформації на хибну. Аналіз представлення інформації в цифровому вигляді: 1) **на один байт припадає** *одна буква, цифра чи символ*; **одне слово може займати** *в мові від 1 до 20 букв*; 3) **кожній букві, цифрі і символу** *присвоєні двійкові коди.* Таблиця кодів складається так, що зникнення чи поява одної 1 в розрядах призводить до зміни одної букви (символу, цифри) на іншу. В цьому випадку проявляється ***однократна помилка***, яка відносно легко виявляється простими засобами апаратного контролю (наприклад, контролем за модулем 2). У випадку ж виникнення ***двократної помилки*** в байті змінитись можуть два розряди. Контроль за модулем 2 цього не виявляє, що вже може призвести до невиявленої зміни одної букви на іншу. В мові існують слова, які змінюють свій зміст на інший при заміні одної букви іншою. Це і є модифікація інформації. При ***трикратній помилці*** імовірність цієї події, природно, збільшується.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Правда, імовірність появи трикратної помилки менша у порівнянні з двократною, але це слабий аргумент, так як її величина при великій кількості апаратних засобів, інтенсивності і накопиченні їх відмов може бути досить відчутною на великому відтинку часу роботи обчислювальної системи.

Якщо розглядати спотворення інформації (без її модифікації) як руйнування інформації, умовою його виникнення може рахуватись однократна помилка, не дивлячись на те, що пропажа однієї букви не завжди спричиняє втрату інформації.

Для виявлення випадкового витоку інформації при її обробці в обчислювальній системі необхідно, щоб в результаті випадкових впливів був переплутаний адрес одержувача чи в правильний адрес була видана інша інформація, що для нього не призначена. В першому випадку, наприклад, замінилась одна з букв іншою (модифікація), в другому - адресація комірок пам’яті ОЗП, з якого зчитувалась інформація до її передачі одержувачу (теж модифікація).

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Витік інформації *- це частковий випадок її модифікації.* **Засоби ФК** використовуються для захисту інформації від випадкових руйнувань, модифікації і витоку. Розглядаючи імовірність появи цих подій при відсутності ФК, зауважимо, що для руйнування інформації (якої-небудь її частини) достатньо однократної помилки, для модифікації і витоку необхідні додаткові умови. Для настання події, що полягає у випадковому роздрукуванні чи відображенні інформації на засобах, які не призначені для цієї мети, необхідно, щоб з потоку помилок виникла така, при якій яка-небудь команда змінилась на команду друк чи відображення, і по санкціонованій команді інформація була б взята не по тому адресу з пам’яті чи була направлена не на той технічний засіб системи. Можливі і інші ситуації. Для настання події, що полягає в модифікації інформації, необхідно щоб з потоку помилок появилась така помилка чи група помилок, завдяки яким справжня інформація змінилась би на хибну, була б не виявлена і підпадала б під подальшу обробку.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Імовірність руйнування інформації від випадкових впливів більша, ніж її модифікація. **Імовірність модифікації інформації більша імовірності її витоку.** Ця оцінка необхідна для вироблення підходу до функціонального контролю з позиції захисту інформації, який полягає у пред’явленні до засобів ФК додаткових вимог, виконання яких може вимагати додаткових засобів. **Додаткові вимоги полягають в реалізації зменшення імовірності модифікації і витоку інформації існуючими засобами підвищення надійності і достовірності інформації.** Для цього використовуються спеціальні схемотехнічні рішення:

1) ізоляція зон доступу до інформації;

2) спеціальна організація роботи з даними, що зберігаються в пам’яті обчислювальної системи.

Ізоляція зон доступу до інформації обчислювальної системи здійснюється також з метою підтримки розмежування санкціонованого доступу.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

З метою вилучення несанкціонованого обміну між користувачами рекомендується при проектуванні зводити до мінімуму число загальних для них параметрів і характеристик механізму захисту. Не дивлячись на те, що функції операційної системи і системи дозволу доступу перекриваються, система доступу повинна конструюватись, як ізольований програмний модуль, тобто захист повинен бути відділений від функцій управління даними. Виконання цього принципу дозволяє програмувати систему дозволу доступу як автономний пакет програм з подальшим незалежним відлагодженням і перевіркою. Даний пакет програм повинен розташовуватись в захищеному полі пам’яті, щоб забезпечити системну локалізацію спроб проникнення зовні. Будь-яка спроба проникнення зі сторони, у тому числі операційної системи, повинна автоматично фіксуватись, документуватись і відхилятись, якщо виклик не передбачений. Природно, що реалізація окремого механізму захисту вимагає збільшення об’ємів програм. При цьому, може виникнути дублювання керуючих і допоміжних програм, а також необхідність в розробленні самостійних функцій, що викликаються.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Інформація, що міститься в обчислювальній системі, може бути поділена між користувачами, що вимагає розміщення її в областях, що не перетинаються, відведених для її зберігання. В кожній з цих областей зберігається сукупність інформаційних об’єктів, що підлягають в рівному ступені захисту. В процесі експлуатації системи необхідно забезпечити надійне розмежування доступу до інформації. Для цієї мети окрім організації доступу з допомогою системи паролів в систему при проектуванні закладаються додаткові міри по ізоляції областей доступу, порушення яких з причини відмов і програмних помилок не спричиняло б несанкціонованого доступу до інформації. До таких мір відносяться організація звертань процесора до пам’яті через регістр дескриптора, вміст якого визначає межі доступної в даний момент області пам’яті шляхом завдання адресів її початку і кінця. Таким чином, вміст регістра є описом (дескриптором) програми, так як вона задає розташування об’єкту в пам’яті. Завдяки тому, що всі звертання до пам’яті проходять через блок перевірки дескрипторів, створюється деякий бар’єр.

Лекція 4
Гарантоздатність автоматизованих систем

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

У випадку наявності в системі загального поля пам’яті, яке необхідне для вирішення поставлених задач, схема захисту допускає обмін інформацією між користувачами. ***Використовуються спискові і мандатні схеми захисту.*** ***Спискові схеми*** - ті, в яких система охорони має список всіх осіб, що мають право доступу до інформації (для отримання права доступу достатньо пред’явити свій ідентифікатор). ***Мандатні схеми*** - ті, в яких система охорони реалізує тільки один вид мандату, а користувач повинен мати набір мандатів для доступу до кожного з необхідних йому об’єктів.

В спискових схемах при кожному звертанні перегляд списку повторюється, тобто доступ пов’язаний з процедурою асоціативного пошуку. В мандатних схемах користувач сам вирішує, який об’єкт йому потрібний, і вибирає необхідний мандат чи деяку їх кількість з тих, до яких він допущений.

Роздільний підхід до захисту інформації від цілеспрямованих і випадкових НСД, що пропонується, передбачає віднести багато вже відомих окремих спеціальних технічних рішень по захисту до засобів захисту від випадкових впливів. До них можна віднести спеціальні засоби захисту операційної системи і пам’яті, що наведені вище.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Особливості вимог до засобів ФК і підвищення достовірності з позиції захисту інформації від НСД:

1) певна цілеспрямованість заходів по ФК і підвищенню достовірності, що виражається у зв’язку технічного представлення інформації і її змістом;
2) визначення залежності безпеки інформації від кратності помилок при її обробці.

Найбільшу небезпеку складають багатократні помилки, які спричиняють модифікацію самої інформації і команд, що здійснюють її обробку. При цьому рівень безпеки інформації є в прямій залежності від кількості помилок, що виникають одночасно. ***Здатність засобів ФК до їх виявлення і визначає рівень безпеки інформації.*** Оскільки імовірність появи чотирикратної помилки відносно мала, то імовірність виявлення дво- і трикратних помилок і буде мірою безпеки інформації на рівні відмов апаратури. На сьогодні є проблема з програмними помилками, що закладені ще на етапі проектування програмного забезпечення (ПЗ).

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Ведуться дослідження щодо підвищення надійності ПЗ. Аналіз наведених засобів ФК і підвищення достовірності інформації, а також спеціальних технічних рішень показує, що із збільшенням кількості байтів в слові імовірність його модифікації від випадкових впливів зменшується, так як збільшується кодова відстань по відношенню до других слів, команд, повідомлень. В цьому розумінні найменш стійкими є короткі слова і особливо цифри. Наведений метод захисту від переадресації пам’яті одному адресу присвоює додаткову спеціальну процедуру і код, що, природно, зменшує імовірність випадкового формування такої процедури і звертань по цьому адресу других процедур і команд. **З метою підвищення безпеки інформації і надійності обчислювальної системи передбачають методи кодування символів, команд і адрес (включаючи адрес пристроїв і процесів) *на предмет: 1) збільшення кодової відстані між ними*, 2) *зменшення імовірності перетворення однієї команди чи адреси в інші.***

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 11.
МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИПАДКОВИХ ВПЛИВІВ

Це дозволить не розробляти деякі складні спеціальні програми, які не усувають причини і умови появи випадкових подій, а лише виявляють їх, та й то не завжди і часом в незручний момент часу, тобто коли подія вже відбулась і основна задача по її попередженню не виконана.

Проблема захисту інформації в АСОД від випадкових впливів заслуговує окремих і більш глибоких досліджень. Поки що на рівні КЗА вона вирішується опосередкованим шляхом за рахунок підвищення надійності роботи апаратних засобів і використання тестових програм. Засобами, що безпосередньо вирішують цю задачу, є лише засоби підвищення достовірності інформації при її передаванні каналами зв’язку між віддаленими об’єктами.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 12.
МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АВАРІЙНИХ СИТУАЦІЙ

Захист інформації від аварійних ситуацій полягає в створенні засобів **1) попередження, 2) контролю, 3) організаційних мір по недопущенню НСД на КЗА в умовах відмов його функціонування, відмов системи захисту інформації, системи життєзабезпечення людей на об’єкті розміщення і при виникненні стихійних лих.**

Аварійна ситуація - подія рідкісна (імовірність її появи залежить від багатьох причин, в тому числі не залежних від людини, і ці причини можуть бути взаємопов’язані), захист від неї є необхідним, так як наслідки в результаті її впливу, як правило, можуть бути досить важкими, а втрати - такими що не відновлюються. Витрати на захист від аварійних ситуацій можуть бути відносно малі, а ефект у випадку аварії - великим.

Відмова функціонування КЗА може спричинити відмову системи захисту інформації, може відкрити доступ до її носіїв: магнітних стрічок, барабанів, дисків і т.п., що може привести до цілеспрямованого руйнування, крадіжки чи підміні носія.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 12.
МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД АВАРІЙНИХ СИТУАЦІЙ

Несанкціонований доступ до внутрішнього монтажу апаратури може привести до підключення сторонньої апаратури, руйнування чи зміни принципової електричної схеми.

Відмова систем життєзабезпечення може привести до виходу з ладу обслуговуючого і контролюючого персоналу. Стихійні лиха: пожар, повінь, землетрус, удари блискавки і т.п. - можуть також привести до вказаних вище наслідків. Аварійна ситуація може бути цілеспрямована створена порушником. В останньому випадку використовуються організаційні заходи.

На випадок відмови функціонування КЗА підсистема контролю відкриття апаратури комплектується автономним джерелом живлення. Для виключення безвідновної втрати інформації носії інформації дублюються і зберігаються в окремому віддаленому і безпечному місці. Для захисту від витоку інформація повинна зберігатись в закритому криптографічним способом вигляді. ***З метою своєчасного прийняття мір по захисту системи життєзабезпечення встановлюються відповідні датчики, сигнали з яких поступають на централізовані системи контролю і сигналізації.***

Лекція 4
Гарантоздатність автоматизованих систем

Глава 13.
ОРГАНІЗАЦІЙНІ ЗАХОДИ ПО ЗАХИСТУ ІНФОРМАЦІЇ

Організаційні заходи по захисту по захисту інформації в АСОД полягають в розробці і реалізації адміністративних і організаційно-технічних заходів при підготовці і експлуатації системи.

Організаційні міри, на думку західних спеціалістів, не дивлячись на постійне удосконалення технічних заходів, складають значну частину (50%) системи захисту. Вони використовуються тоді, коли обчислювальна система не може безпосередньо контролювати використання інформації. Крім того, в деяких відповідальних випадках з метою підвищення ефективності захисту корисно іноді технічні засоби продублювати організаційними.

Організаційні заходи по захисту систем в процесі їх функціонування і підготовки до нього охоплюють рішення і процедури, що приймає керівництво організації - споживача системи. Хоча деякі з них можуть визначатись зовнішніми факторами, наприклад законами чи урядовими постановами, більшість проблем вирішуються в середині організації в конкретних умовах.

Складовою частиною будь-якого плану заходів повинна бути чітко сформульована мета, розподіл відповідальності і перелік організаційних заходів захисту.

Глава 13.
ОРГАНІЗАЦІЙНІ ЗАХОДИ ПО ЗАХИСТУ ІНФОРМАЦІЇ

Конкретний розподіл відповідальності і функцій по реалізації захисту від організації до організації може змінюватись, але ретельне планування і точний розподіл відповідальності є необхідною умовою створення ефективної і життєздатної системи захисту.

Організаційні заходи по захисту інформації в системі повинні охоплювати етапи: 1) проектування, 2) розроблення, 3)виготовлення, 4) випробовувань, 5)підготовлення до експлуатації, 6)експлуатацію системи.

У відповідності з вимогами технічного завдання в проектній організації поряд з технічними заходами розробляються і впроваджуються організаційні заходи по захисту інформації на етапі створення системи.

Під етапом створення розуміються проектування, розроблення, виготовлення і випробовування системи. При цьому слід відмітити заходи по захисту інформації, що проводяться організацією-проектувальником, розробником і виготовлювачем в процесі створення системи і розраховані на захист від витоку інформації в даній організації, і заходи, що закладаються в проект і документацію, що розробляється на систему, які стосуються принципів організації захисту.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 13.
ОРГАНІЗАЦІЙНІ ЗАХОДИ ПО ЗАХИСТУ ІНФОРМАЦІЇ

До організаційних заходів по захисту інформації в процесі створення системи відносяться:

-введення на необхідних ділянках проведення робіт з режимом секретності;
- розроблення посадових інструкцій по забезпеченню режиму секретності у відповідності з діючими в країні інструкціями і положеннями;
-при необхідності виділення окремих приміщень з охороною сигналізацією і пропускною системою;
-розмежування задач по виконавцям і випуску документації;
- присвоєння грифу секретності матеріалам, документації, апаратурі і зберігання їх під охороною в окремих приміщеннях з врахуванням і контролем доступу виконавців;
-постійний контроль за дотриманням виконавцем режиму і відповідних інструкцій;
-установлення і розподіл відповідальних осіб за витік інформації т.і.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 14.
ЗАКОНОДАВЧІ ЗАХОДИ ПО ЗАХИСТУ ІНФОРМАЦІЇ

Законодавчі заходи по захисту інформації від НСД полягають у виконанні існуючих в країні чи запровадженні нових законів, положень, постанов і інструкцій, що регулюють юридичну відповідальність посадових осіб - користувачів і персоналу, що обслуговує техніку, за витік, втрату чи модифікацію інформації, що підлягає захисту і довірена йому, у тому числі за спробу виконати аналогічні дії за межам своїх повноважень, а також відповідальності сторонніх осіб за спробу цілеспрямованого несанкціонованого доступу до апаратури і інформації.

Мета законодавчих заходів - попередження і стримування потенційних порушників.

Лекція 4
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.1. Аналіз розвитку концепції захисту інформації в АСОД

Розвиток концептуальних підходів до створення захисту інформації в автоматизованих системах сьогодні є актуальним з точки зору використання (створення) надійних механізмів забезпечення безпеки, які складаються в основному з технічних і програмних засобів.

Технічні засоби реалізуються, як: 1) електричні, 2) електромеханічні; 3) електронні пристрої.

Сукупність технічних засобів було прийнято ділити на апаратні і фізичні (див. системна модель безпеки ІТ).

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Апаратні технічні засоби захисту – це пристрої, що вбудовуються безпосередньо в апаратуру АСОД, чи пристрої, що стикуються з апаратурою АСОД по стандартному інтерфейсу.

Фізичні засоби реалізуються у вигляді автономних пристроїв і систем (електронно-механічне обладнання охоронної сигналізації і спостереження, замки на дверях, грати на вікнах і т.і.).

Програмні засоби захисту - це програми, спеціально призначені для виконання функцій, пов’язаних із захистом інформації.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

На першому етапі проектування захисту інформації в автоматизованих системах (60-і роки) серед перерахованих трьох основними засобами були програмні, як такі, що працюють ефективно, за умови включення їх до складу загальносистемних компонентів програмного забезпечення.

Програмні механізми захисту включались до складу операційних систем або систем управління базами даних, але на практиці виявлено, що надійність механізмів захисту такого типу є недостатньою.

Лекція 5
Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Кроком на шляху до підвищення ефективності програмного захисту стала **організація диференційованого розмежування доступу користувачів до даних,** що знаходяться в АСОД.

Алгоритм: 1) ідентифікація всіх користувачів та всіх елементів даних, що захищаються; 2) встановлення відповідності між ідентифікаторами користувачів і ідентифікаторами елементів даних; 3) побудова алгоритмічної процедури перевірки кожного запиту користувача.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Наступний крок – створення системи безпеки ресурсу в операційній системі (фірма IBM), яка здатна реалізувати три основні функції захисту: 1) ізоляцію; 2) контроль доступу; 3) контроль рівня захисту. У такій системі програмний захист доповнюється комплексом організаційних мір.

Висновок: концепція захисту на основі механізмів безпеки в рамках операційної системи, не відповідає вимогам надійності.

Для подолання недоліків перспективними були рішення:

1) **створення** в механізмах захисту - **ядра безпеки**; 2) **децентралізація механізмів захисту**, аж до створення елементів, що знаходяться під керуванням користувачів АСОД; 3) **розширення арсеналу засобів захисту.**

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Другий етап розвитку концепції захисту інформації в АСОД (70-і роки): розвиток технічних і криптографічних засобів.

Третій етап (80-і роки) розвитку концепції захисту інформації: **застосування системного підходу до проблеми захисту інформації.**

Характреристика етапу:

Застосування системності на рівнях:

а) створення відповідних механізмів захисту;

б) забезпечення регулярності процесу безпеки на усіх етапах життєвого циклу АСОД при комплексному використанні всіх засобів захисту.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Системний підхід передбачає: об’єднання всіх засобів, методів, заходів, що використовуються для захисту інформації, обов’язково в єдиний цілісний механізм - систему захисту.

Склад системи захисту – чотири захисних пояси (див. аналог - комплексну модель захисту ІТ) :

1) зовнішній пояс, що охоплює всю територію, на якій розташовані споруди АСОД;
2) пояс споруд, приміщень чи пристроїв АСОД;
3) пояс компонентів системи (технічних засобів, програмного забезпечення, елементів баз даних);
4) пояс технологічних процесів обробки даних (введення/виведення, внутрішня обробка і т.і.).

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Реалізація системного підходу до захисту інформації – **проект системи захисту, що враховує такі положення:**

1) система захисту інформації розробляється і впроваджується одночасно з розробленням самої АСОД;
2) реалізація функції захисту - в основному апаратна;
3) забезпечення рівня захисту, який задається.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Проблема захисту програмного забезпечення АСОД обумовлена:

1) програмне забезпечення відіграє вирішальну роль в якісній обробці інформації;
2) програми є предметом комерційної таємниці;
3) програмні засоби є одними з найбільш вразливих компонентів АСОД. **Особливими є елементи загроз, що пов’язані з комп’ютерними вірусами.**

Лекція 5
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

З метою забезпечення захисту інформації в АСОД на основі системного підходу розглядають:

- **перший** напрям, який орієнтований на обчислювальні мережі;
- **другий** напрям, спрямований на територіально-зосереджені АСОД та організацію робіт із захисту інформації при їх проектуванні і розробленні.

Характеристика предмету захисту - інформаційних ресурсів: 1) множина предметів захисту; 2) множина потенційних загроз цим ресурсам;
3) адекватна множина засобів захисту.

1) **Інформаційні ресурси** – запаси чого-небудь: об’ємів пам’яті, часу функціонування, швидкодії і т.і. (Енциклопедичний словник).

До складу ресурсів включені: 1) всі компоненти обчислювальної мережі, 2) її апаратне і програмне забезпечення, 3) процедури, протоколи, управляючі структури і т.і. 2) **Інформаційні ресурси** – інформація, яка представляє цінність для підприємства і може бути оцінена подібно матеріальним ресурсам (Тлумачний словник з обчислювальної техніки і програмування).

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Основні визначення термінів в контексті побудови системи захисту на основі системного підходу:

а) **система захисту даних** - комплекс апаратних, програмних і криптографічних засобів, а також заходи, що забезпечують захист даних від випадкового чи цілеспрямованого руйнування, спотворення чи використання;

б) **система захисту інформації від несанкціонованого доступу** - комплекс організаційних мір і програмно-технічних (в тому числі криптографічних) засобів захисту від несанкціонованого доступу до інформації в автоматизованих системах;

в) **система захисту секретної інформації** - комплекс організаційних мір і програмно-технічних (у тому числі криптографічних заходів) засобів забезпечення безпеки інформації в автоматизованих системах;

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

г) **засоби захисту від несанкціонованого доступу** - програмні, технічні чи програмно-технічні, призначені для запобігання чи істотного утруднення несанкціонованого доступу;

д) **захищена система** – система, вхід до якої вимагає введення паролю;

е) **суб’єкт безпеки** - активна системна складова, в якій використовується відповідна методика безпеки

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

ж) **суб’єкт доступу** - особа чи процес, дія яких регламентується правилами розмежування доступу;

з) **безпека інформації** - стан захищеності інформації, що обробляється засобами обчислювальної техніки чи автоматизованої системи, від внутрішніх чи зовнішніх загроз.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Згідно розглянутих визначень:

а) **безпека АСОІ** – властивості системи, що полягають в здатності протидіяти спробам нанесення шкоди власникам чи користувачам системи при різноманітних навмисних і ненавмисних впливах на неї;

б) **система захисту АСОІ** – єдина сукупність правових і морально-етичних норм, організаційних (адміністративних) мір і програмно-технічних засобів, направлених на протидію загрозам АСОІ з метою зведення до мінімуму можливої шкоди користувачам чи власникам системи.

Відповідно:

а) **захист інформаційних ресурсів обчислювальної мережі**: всі операції з цими ресурсами виконуються за чітко визначеними правилами та інструкціями;

б) **система захисту обчислювальної мережі** визначена у формі списків, процедур і засобів захисту.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Визначення:

а) **суб’єкт доступу** - особа чи процес, дія якого регламентується правилами розмежування доступу;

б) **об’єкт доступу** - одиниця інформаційного ресурсу автоматизованої системи, доступ до якої регламентується правилами розмежування доступу;

в) **захищений засіб обчислювальної техніки (захищена автоматизована система)** - засіб обчислювальної техніки (автоматизованої системи), в якому реалізований комплекс засобів захисту;

г) **концепція диспетчера доступу** - концепція управління доступом, що відноситься до абстрактної машини, яка здійснює посередницькі операції при всіх звертаннях суб’єктів до об’єктів.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

З аналізу попереднього матеріалу:

1) відсутність чітких і зрозумілих визначень об’єктів і предмету захисту;

2) відсутність оптимальних класифікацій потенційних загроз і можливих каналів НСД;

3) відсутність адекватних моделей об’єкту захисту інформації та очікуваної моделі поведінки порушника.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Поділ окремих засобів захисту на апаратні, фізичні, програмні, інженерні та інші, який покладено в основу принципів побудови системи захисту, **не враховує функціональні можливості при їх взаємодії та створює передумови для утворення щілин у захисті.**

При побудові захисту часто не враховується – відмінність предметів захисту, можливих каналів НСД і відповідних засобів захисту на етапах проектування і експлуатації АСОД.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Потрібна чітка та обгрунтована класифікація об’єктів захисту інформації за принципами побудови, яка б дозволяла знайти єдиний підхід до захисту територіально-зосереджених і глобальних АСОД.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Потрібне представлення потенційних загроз, що повністю враховує їх фізичне походження і точки прикладення в обчислювальній системі (наприклад, різну природу випадкових і цілеспрямованих впливів).

У разі відсутності: недостатньо точно визначені можливі підходи порушника до об’єкту захисту, що, в свою чергу, не дозволяє встановити на його шляху відповідні перепони.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Потрібне обгрунтування та реалізація принципу рівної міцності ланок захисту. який випливає із необхідності створення навколо предмета захисту замкненої лінії безпеки.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.2. Аналіз видів автоматизованих систем обробки інформації і вибір загального підходу до побудови системи її безпеки

Проблема безпеки інформації в автоматизованих систем її обробки: від персонального комп’ютера і великих обчислювальних комплексів до глобальних обчислювальних мереж і АСУ різного призначення.

Задачі: 1) створення систем забезпечення: надійності функціонування автоматизованих систем, стійкості до зовнішніх впливів, швидкості обробки даних; 2) створені системи повинні забезпечувати гарантовану безпеку інформації, що обробляється.

Лекція 5
Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

АСОД поділяються на два види: з централізованою і децентралізованою обробкою даних.

До централізованої відносяться: 1) ЕОМ; 2) обчислювальні комплекси; 3) обчислювальні системи.

Обчислювальні системи можуть містити в своєму складі обчислювальні комплекси і ЕОМ.

АСУ - обчислювальні системи, що з’єднані через обчислювальну мережу каналами зв’язку.

Обчислювальна мережа складається з обчислювальних систем, що з’єднані між собою каналами зв’язку.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Обчислювальну систему з позицій безпеки інформації можна розглядати, як деякий базовий елемент **обчислювальної мережі та АСУ.**

Узагальнена функціональна схема такої обчислювальної системи представлена на рис. 16.1а.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

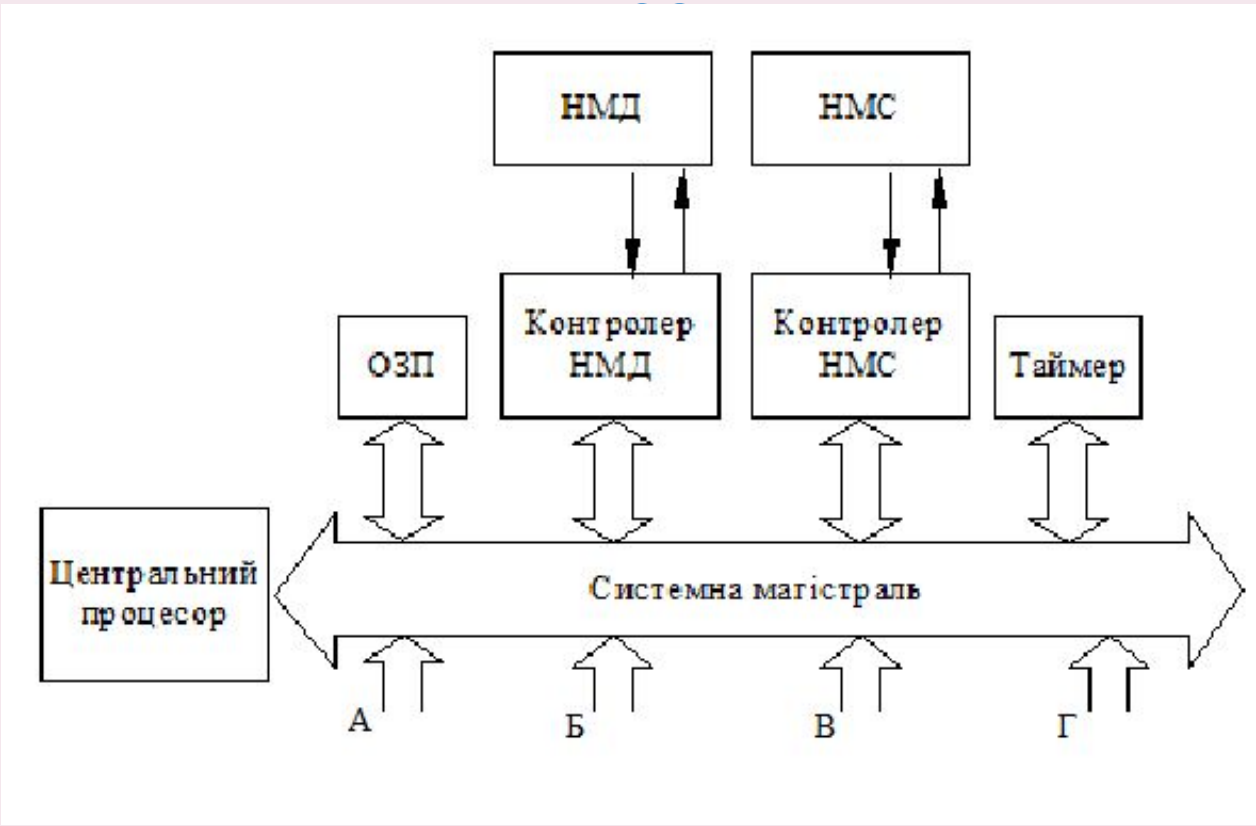


Рис 16.1а

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

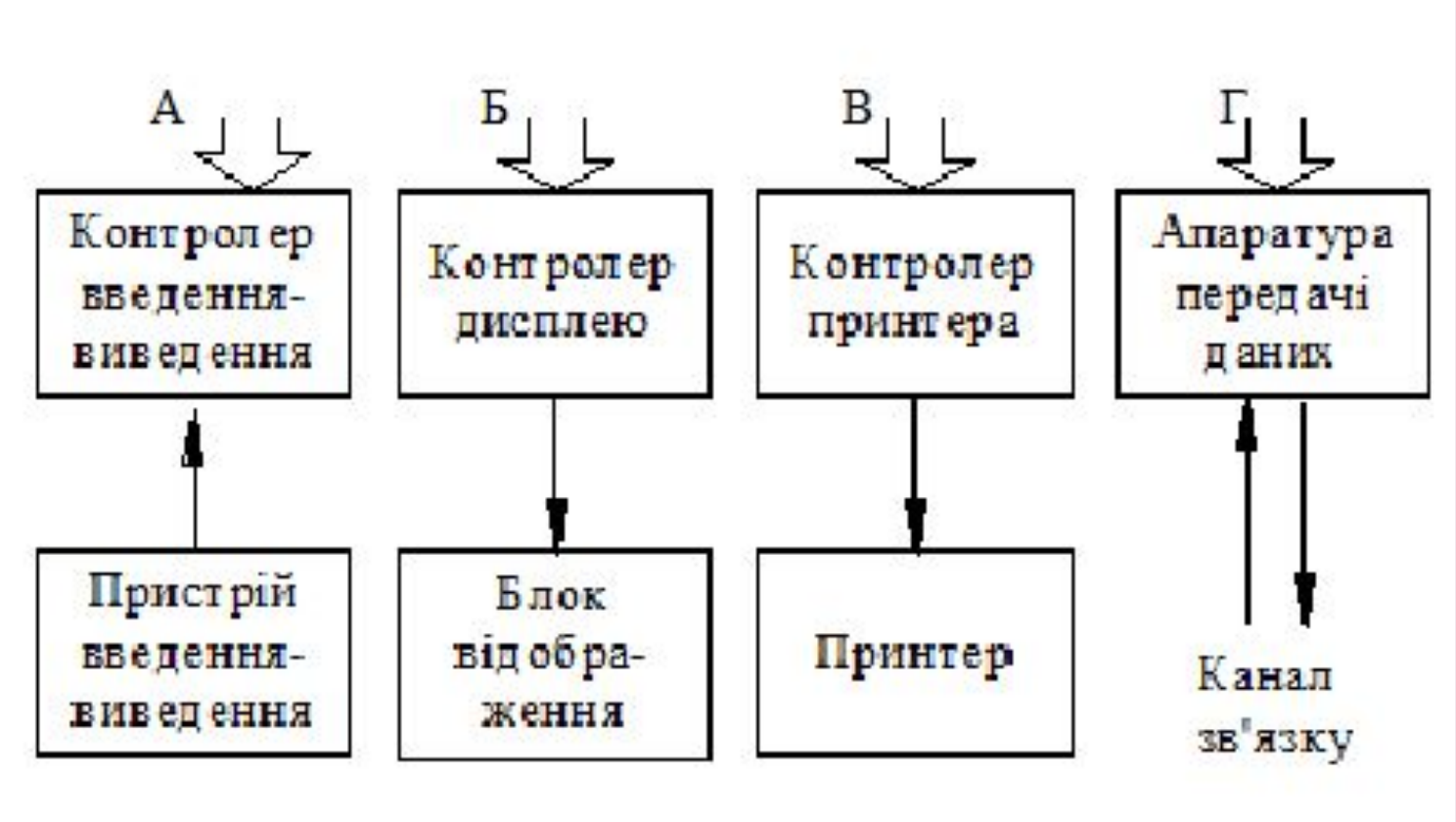


Рис 16.1а (Обч. система = обч. мережа + АСУ (продовж.))

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Загальний підхід до розробки концепції безпеки інформації для вказаних АСОД полягає в: 1) аналізі цього елемента; 2) розробці концептуальних основ захисту інформації на його рівні; 3) розробці захисту на рівні обчислювальної мережі і АСУ. **Підхід характерний:** 1) переходом від простого до складного; 2) дозволяє отримати можливість розповсюдження отриманих результатів на персональну ЕОМ і локальну обчислювальну мережу, розглядаючи першу як АСОД з централізованою, а другу - з децентралізованою обробкою даних.

Для представлення АСОД з децентралізованою обробкою даних використовується комплекс засобів автоматизації (КЗА) обробки даних, що включає: обчислювальну систему, або локальну обчислювальну мережу, або їх поєднання, або декілька таких систем. На рис. 16. 1 б – узагальнена структура АСУ.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

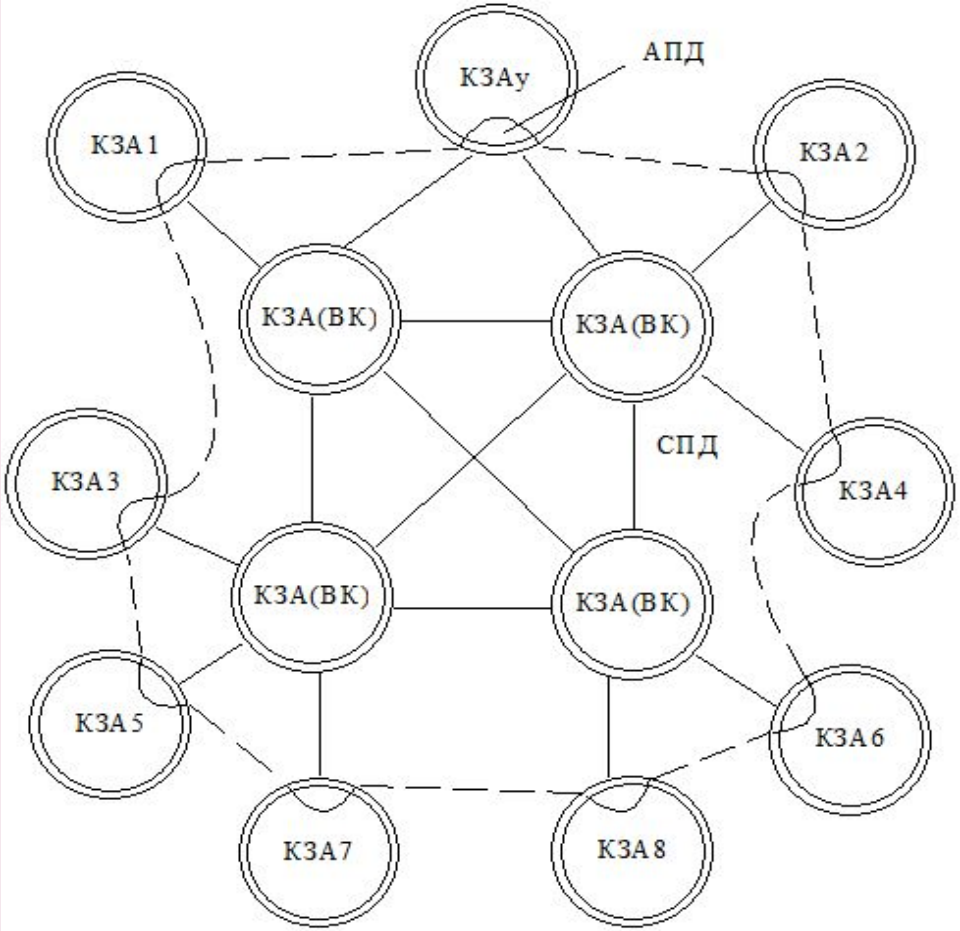


Рис. 16.1б. Узагальнена структура АСУ

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.3. Основи теорії захисту інформації від несанкціонованого доступу

Модель поведінки потенційного порушника

Порушення – спроба несанкціонованого доступу (НСД) до будь-якої частини інформації, що підлягає захисту, зберігається, обробляється і передається в АСУ. Оскільки час і місце цілеспрямованого НСД передбачити неможливо, доцільно створити деяку модель поведінки потенційного порушника, **передбачаючи найбільш небезпечну ситуацію**:

а) **порушник може появитись в будь-який час і в будь-якому місці** перемитра автоматизованої системи;

б) **кваліфікація і обізнаність порушника** може бути на рівні розробника даної системи;

в) **порушнику відома інформація** про принципи роботи системи, включаючи секретну;

г) **порушник вибирає найбільш слабку ланку** в захисті;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

д) **порушником може бути** не тільки стороння особа, але й законний користувач системи;

е) **порушник діє один**.

Основні принципи побудови системи згідно моделі порушника.

Згідно п. а необхідно будувати навколо предмету захисту постійно діючий замкнений контур (чи оболонку) захисту.

Згідно п. б властивості перепони, що складають захист, повинні по можливості відповідати кваліфікації і обізнаності порушника, що очікується.

Згідно п. в для входу в систему законного користувача необхідна змінна секретна інформація відома тільки йому.

Згідно п. г результуюча (сумарна) міцність захисного контуру визначається його найслабшою ланкою.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Згідно п. д при наявності декількох законних користувачів корисно забезпечити розмежування їх доступу до інформації у відповідності з повноваженнями і функціями, що виконуються, реалізуючи таким чином принцип найменшої обізнаності кожного користувача з метою скорочення збитків у випадку, якщо має місце безвідповідальність одного з них.

Згідно п. е в якості вихідної передумови також рахуємо, що порушник один, оскільки захист від групи порушників (що виконують одну задачу під єдиним керівництвом) – задача окремого дослідження.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Для різних АСОД: **за призначенням і принципами побудови; видом і цінністю інформації, що в них оброблюється**, найбільш небезпечна модель поведінки потенційного порушника також може бути різною. Для військових систем це рівень розвідника-професіонала, для комерційних систем - рівень кваліфікованого користувача і т.д. Для медичних систем, наприклад скоріш за все не буде потрібним захист від побічного електромагнітного випромінювання і наводок, але захист від безвідповідальності користувачів просто необхідний. Очевидно, що для захисту інформації від більш кваліфікованого і обізнаного порушника необхідно буде розглянути більшу кількість можливих каналів НСД і використати більшу кількість засобів захисту з більш високими показниками міцності.

На основі викладеного для вибору вихідної моделі поведінки потенційного порушника доцільний диференційований підхід. За основу прийнято чотири класи безпеки:

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

- 1-й клас рекомендується для захисту життєво важливої інформації, витік, руйнування чи модифікація якої можуть призвести до великих втрат для користувачів. **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 чи формуючих свої файли, що недоступні іншим користувачам. **Міцність захисту повинна бути розрахована на порушника високої кваліфікації, але не на зломщика-професіонала.**

- 3-й клас рекомендується для захисту відносно цінної інформації, постійний несанкціонований доступ до якої шляхом її накопичення може привести до витоку і більш цінної 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.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Реалізація перерахованих рівнів безпеки повинна забезпечуватись комплексом відповідних засобів захисту, що перекривають певну кількість каналів НСД у відповідності до класу очікуваних потенційних порушників. **Рівень безпеки інформації всередині класу** забезпечується кількісною оцінкою міцності окремих засобів захисту і оцінкою міцності контуру захисту від цілеспрямованого НСД за розрахунковими формулами (далі).

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

1. МОДЕЛЬ ЕЛЕМЕНТАРНОГО ЗАХИСТУ

В загальному випадку найпростіша модель елементарного захисту будь-якого предмету може бути у вигляді, що представлений на рис. 16.2.

Предмет захисту розміщений в замкненій і однорідній захисній оболонці, що називається **перепоною**. Міцність захисту залежить від властивостей перепони. Принципову роль грає здатність перепони протистояти спробам її подолання порушником. Властивість предмету захисту – здатність приваблювати його власника і потенційного порушника. Притягальна сила предмету захисту полягає в його ціні. Ця властивість предмету захисту широко використовується при оцінці захищеності інформації в обчислювальних системах. **Міцність створеної перепони достатня, якщо вартість прогнозованих затрат на її подолання потенційним порушником перевищує вартість інформації, що захищається.**

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

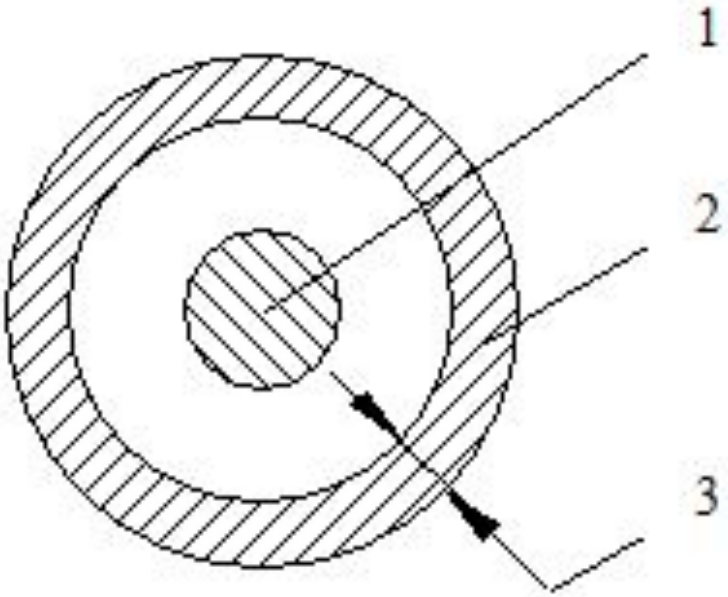


Рис. 16.2. Модель елементарного захисту:
1 - предмет захисту;
2 - перепона;
3 - міцність перепони

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Однак можливий і інший підхід.

Відомо, що інформація з часом губить свою привабливість і починає старіти, а в окремих випадках її ціна може впасти до нуля. Тоді, **за умову достатності захисту** можна прийняти перевищення затрат часу на подолання перепони порушником над часом життя інформації. **1)** Якщо позначити імовірність не подолання перепони порушником $P_{ЗІ}$, час життя інформації через $t_ж$ очікуваний час подолання перепони порушником через $t_п$, імовірність обходу перепони порушником через $P_{об\ х}$, то для випадку старіння інформації **умову достатності захисту** отримаємо у вигляді наступних співвідношень:

$$P_{ЗІ} = 1, якщо\ \ \mathrm{t_ж} < t_п \ \mathrm{і}\ \mathrm{P_{обх}} = 0$$

$P_{об\ х}$ рівне нулю, означає необхідність замикання перепони навколо предмету захисту.**2)** Якщо $t_ж > t_п$, $а\ \mathrm{P_{обх}} = 0$, $то$ $P_{зі} = (1 - P_{пр})$

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

$P_{пр}$ де – імовірність подолання перепони порушником за час, менший $t_{ж}$.

3) Для реального випадку, коли $t_{ж} > t_{п}$, $P_{обх} > 0$ **міцність захисту** можна представити у вигляді:

$$P_{зі} = (1 - P_{пр})(1 - P_{обх})$$

де $P_{пр} = 0$, ;якщо $t_{ж} < t_{п}$, $P_{пр} > 0$, якщо $t_{ж} > t_{п}$.

Ця формула справедлива для випадку коли порушників двоє, тобто коли один долає перепону, а інший її обходить. В початковій моделі поведінки потенційного порушника: порушник буде один і йому відомі міцність перепони і складність шляхів її обходу. Оскільки одночасно двома шляхами він іти не зможе, він вибере один з них – найбільш простий, тобто за формулою. Тоді формальний вираз міцності захисту в цілому для даного випадку буде відповідати формулі:

$$P_{зі} = (1 - P_{пр}) \cup (1 - P_{обх})$$

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

де – $\cup$ знак АБО

В якості прикладу елементарного захисту, що розраховується за формулою може бути названий криптографічний захист інформації, де величина P_{np} може визначатись шляхом оцінки імовірності підбору коду ключа, з допомогою якого можна дешифрувати закриту даним способом інформацію. Згідно трактування цю величину можна визначити за формулою

$$P_{np} = \frac{n}{A^s}$$

де **n** - кількість спроб підбору коду; **A** – число символів у вибраному алфавіті коду ключа; **S** – довжина коду ключа в кількості символів.

Величина буде залежати від: 1) вибраного методу шифрування, 2) способу використання, 3) повноти перекриття тексту інформації, 4) існуючих методів криптоаналізу, 5) способу зберігання дійсного значення коду ключа і періодичності його заміни на нові значення, якщо інформація закрита даним способом, постійно зберігається у її власника.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

4) Можливо також, що у однієї перепони може бути декілька шляхів обходу. Тоді формула приймає вигляд:

$$P = (1 - P_{пр}) \cup (1 - P_{обх\ 1}) \cup (1 - P_{обх\ 2}) \cup \ldots \cup (1 - P_{обх\ К})$$

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

$$1 - P_{пр}\ ,\ 1 - P_{обх\ 1}\ ,\ 1 - P_{обх\ 2}\ ,\ 1 - P_{обх\ К}$$

Принцип роботи автоматизованої перепони базується на тому, що в ній блоком управління виконується періодичний контроль датчиків виявлення порушника. Результати контролю спостерігаються людиною. Періодичність опитування датчиків автоматом може досягати тисячних часток секунди і менше. У цьому випадку очікуваний час подолання перепони порушником значно перевищує період опитування датчиків. Тому такий контроль часто рахують постійним.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Але для виявлення порушника людиною, що керує автоматом контролю, тільки малого періоду опиту датчиків недостатньо.

Необхідний ще й **час на вироблення сигналу тривожної сигналізації**, тобто час спрацювання автомату, оскільки він часто значно перевищує період опитування датчиків і тим самим збільшує час виявлення порушника. Практика показує, що звичайно сигналу тривожної сигналізації достатньо для припинення дій порушника, якщо цей сигнал до нього дійшов. Але оскільки фізичний доступ до об’єкту захисту поки ще відкритий, подальші дії охорони зводяться до визначення місця і організації блокування доступу порушника, на що так само потрібний час.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

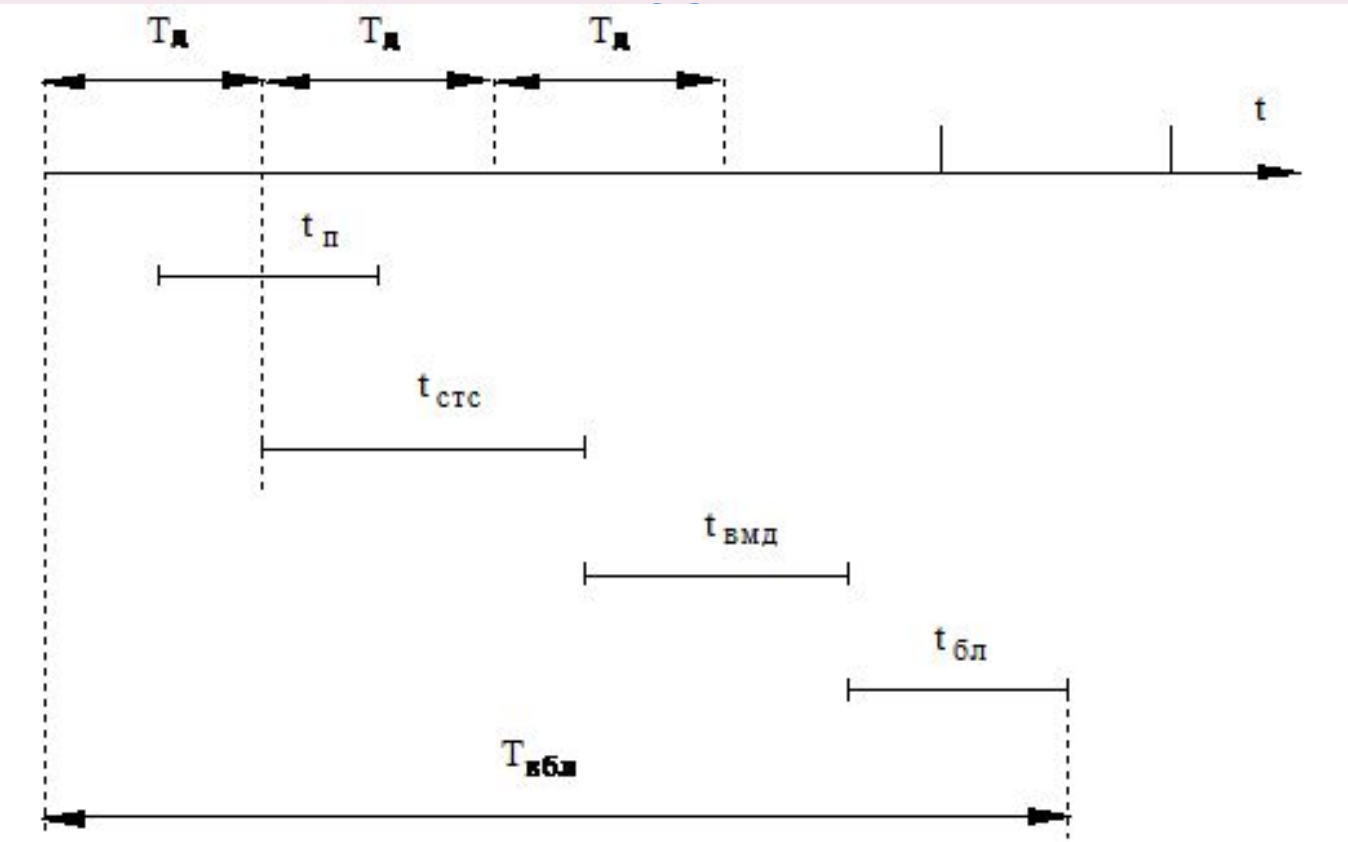


Рис. 16.3. Часові діаграми контролю НСД

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Таким чином, умову міцності перепони з виявленням і блокуванням НСД можна представити у вигляді співвідношення:

$$\frac{T_д + t_{стс} + t_{вмд} + t_{бл}}{t_g} > 1$$

Де $T_д$ – період опитування датчиків; $t_{стс}$ – час спрацювання тривожної сигналізації; $t_{вмд}$ – час виявлення місця доступу; $t_{бл}$ – час блокування доступу.
Якщо позначимо чисельник через $T_{вбл}$, отримаємо співвідношення:

$$\frac{T_{вбл}}{t_n} < 1$$

де $T_{вбл}$ – час виявлення і блокування несанкціонованого доступу.
Процес контролю НСД і несанкціонованих дій порушника в часі наведений на рис. 16.3.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Із діаграми на рис. 16.3. випливає, що порушник може бути **не виявлений** в двох випадках:

а) коли $t < T_д$;

б) коли $T_д < t_п < T_{вбл}$.

В першому випадку необхідна додаткова умова – попадання інтервалу часу в інтервал $T_д$, тобто необхідна синхронізація дій порушника з частотою опитування датчиків виявлення. Для вирішення цієї задачі порушнику доведеться непомітно підключити вимірювальну апаратуру в момент виконання несанкціонованого доступу до інформації, що є достатньо складною задачею для сторонньої людини. Тому рахуємо, що свої дії з частотою опитування датчиків він синхронізувати не зможе і може розраховувати лише на деяку імовірність успіху, яка залежить від імовірності попадання відрізку часу в проміжок часу між імпульсами опитування датчиків.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Імовірність успіху порушника:

$$P_n = \frac{T_д - t_n}{T_д} = 1 - \frac{t_n}{T_д}$$

А) Імовірність виявлення несанкціонованих дій порушника:

$$P_в = 1 - P_{пр}$$

або

$$P = \frac{t_n}{T_д}$$

При $t_n > T_д$ порушник буде виявлений обов’язково. В другому випадку імовірність успіху порушника буде визначатись за аналогією із попереднім співвідношенням:

$$P_{пр} = 1 - \frac{t_n}{T_{вбл}}$$

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Б) Імовірність виявлення і блокування несанкціонованої дії порушника:

$$P_{вбл} = (1 - P_{пр})$$

$$P_{вбл} = \frac{t_n}{T_{вбл}}$$

При $t_n > T_{вбл}$ спроба НСД не має змісту, так як вона буде виявлена обов’язково. В цьому випадку $P_{вбл} = 1$.

1. Міцність перепони з властивостями виявлення і блокування *:

$$P_{зі_k} = P_{вбл}(1 - P_{від}) \cup (1 - P_{обх_1}) \cup (1 - P_{обх_2}) \cup \ldots \cup (1 - P_{обх_j})$$

де **j** – число шляхів обходу цієї перепони; $\cup$ – знак АБО.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Слід також відзначити, що ця формула справедлива також і для організаційного заходу захисту у вигляді періодичного контролю заданого об’єкту людиною. При цьому вважаємо, що виявлення, визначення місця НСД і його блокування відбувається в один час – в момент контролю об’єкта людиною, тобто $t_{стс} = t_{вмд} = t_{бл} = 0$, $T_{вбл} = T$ де Т – період контролю людиною об’єкта захисту.

Для більш повного представлення міцності перепони **у вигляді автоматизованої системи виявлення і блокування НСД** необхідно враховувати надійність її функціонування і шляхи можливого обходу її порушником. Імовірність відмови системи визначається за відомою формулою:

$$P_{від}(t) = e^{-\lambda t}$$

де λ – інтенсивність відмов групи технічних засобів, що складають систему виявлення і блокування НСД; **t** – інтервал часу функціонування системи виявлення і блокування НСД, що розглядається.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

2. Міцність перепони з врахуванням можливої відмови системи контролю:

$$P_{зі_k} = P_{вбл}(1 - P_{від}) \cdot (1 - P_{обх_1}) \cdot (1 - P_{обх_2}) \cdot \ldots \cdot (1 - P_{обх_j})$$

де $P_{вбл}$, $P_{від}$ визначаються відповідно за формулами;
кількість шляхів обходу **j** визначаються експертним шляхом на основі аналізу принципів побудови системи контролю і блокуванню НСД.

Одним з можливих шляхів обходу системи виявлення і блокування може бути можливість непомітного відключення порушником системи виявлення і блокування (наприклад, шляхом обриву чи замикання контрольних кіл, підключенням імітатора контрольного сигналу, зміни програми збирання сигналів і т.п.). Імовірність такого роду подій визначається в межах від 0 до 1 методом експертних оцінок на основі аналізу принципів побудови і роботи системи. При відсутності можливості несанкціонованого відключення системи величина її імовірності дорівнює нулю.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

2. МОДЕЛЬ БАГАТОЛАНКОВОГО ЗАХИСТУ

На практиці в більшості випадків захисний контур складається з декількох з’єднаних між собою перепон з різною міцністю. Модель такого захисту з декількох ланок представлена на рис. 16.4. Прикладом такого виду захисту може бути приміщення, в якому зберігається апаратура. Перепони різної міцності – стіни, стеля, підлога, вікна і замок на двері.

Для обчислювальної системи, модель якої представлена на рис. 16.1, з’єднання перепон (замикання контуру захисту) має той самий зміст, але іншу реалізацію. Система контролю відкриття апаратури і система розпізнавання і розмежування доступу, **які контролюють доступ до периметру обчислювальної системи,** утворюють замкнений захисний контур, але доступ до засобів відображення і документування, до побічного електромагнітного випромінювання і наведень (ПЕМВН), носіїв інформації та інших можливих каналів НСД до інформації **не перекривають**.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

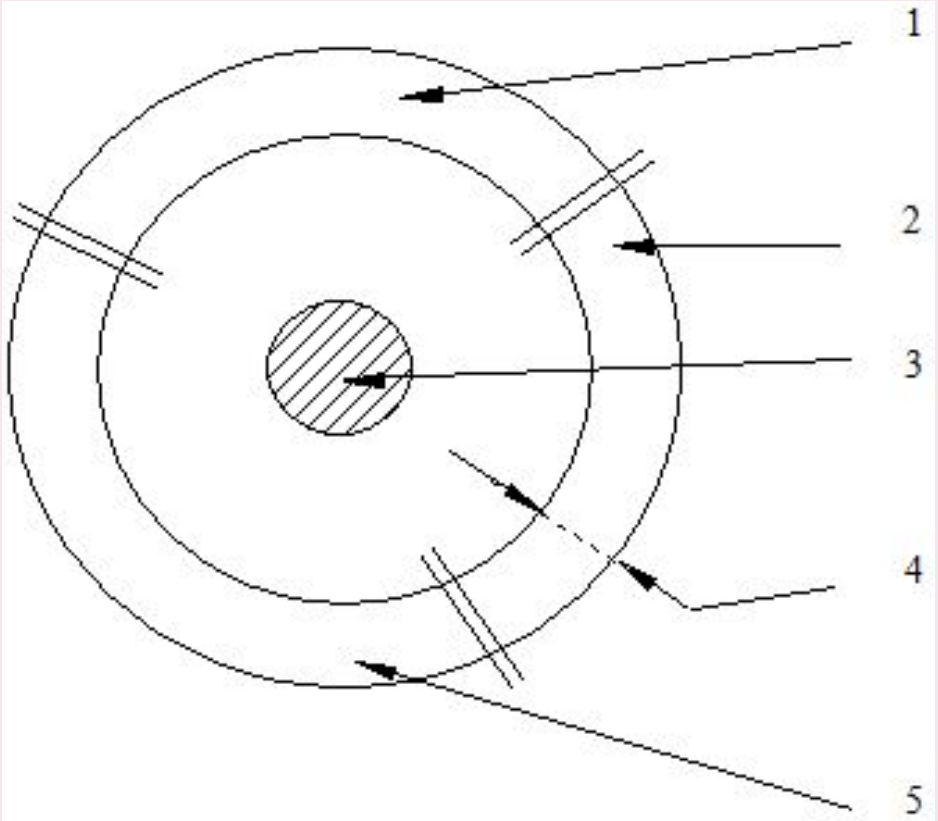


Рис. 16.4. Модель багатоланкового захисту:
1 - препона 1; 2 - перепона 2; 3 - предмет захисту;
4 - міцність перепони; 5 - перепона 3.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

В контур захисту в якості його ланок увійдуть: 1) системи контролю доступу в приміщення, 2) засоби захисту від ПЕМВН, 3) шифрування т.і. Контур захисту не буде замкнений до тих пір, доки існує яка-небудь можливість несанкціонованого доступу до одного й того самого предмету захисту.

1. Міцність багатоланкового захисту при використанні неконтрольованих перепон:

$$P_{зі} = P_{зі_1} \cdot P_{зі_2} \cdot P_{зі_3} \cdot \ldots \cdot P_{зі_i} \cdot (1 - P_{обх_1}) \cdot (1 - P_{обх_2}) \cdot \ldots \cdot (1 - P_{обх_j})$$

Необхідно підкреслити, що розрахунки узагальнених міцностей захисту для неконтрольованих і контрольованих перепон повинні бути окремими, оскільки вихідні дані для них різні, і, отже, це різні задачі для різних контурів захисту.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Якщо міцність найслабшої ланки задовольняє поставленим вимогам до контуру захисту в цілому, виникає питання про надлишковість міцності інших ланок даного контуру. Звідси випливає, що економічно доцільно використовувати в багатоланковому контурі захисту перепони однакової міцності.

При розрахунку міцності контуру захисту з багатьма ланками може статись, що ланка з найменшою міцністю не задовольняє поставленим вимогам. Тоді перепону в цій ланці замінюють на більш міцну чи дана перепона дублюється ще однією перепоною, а іноді двома чи декількома перепонами. Але всі додаткові перепони повинні перекривати ту саму чи більшу кількість каналів НСД, що й перша. **2. Сумарна міцність дубльованих перепон:**

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

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

де **i = 1,...,m** – порядковий номер перепони; **m** – кількість дублюючих перепон; міцність P_i і-ї перепони –

Інколи ділянку захисного контуру з паралельними (продубльованими) перепонами називають **багаторівневим захистом**. В обчислювальній системі захисні перепони часто перекривають одна одну і з причини, що вказана вище, і коли специфіка можливого каналу НСД вимагає використання такого засобу захисту (наприклад, системи контролю доступу а приміщення, охоронної сигналізації і контрольно-пропускного пункту на території об’єкта захисту). Це означає, що міцність окремої перепони , що попадає під захист другої, третьої і т.д. перепони, повинна перераховуватись з врахуванням цих перепон. Відповідно може змінитись і міцність найслабшої перепони, що визначає результуючу міцність захисного контуру в цілому.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

3. МОДЕЛЬ БАГАТОРІВНЕВОГО ЗАХИСТУ

У відповідальних випадках при підвищених вимогах до захисту використовується **багаторівневий захист**, модель якого наведена на рис. 16.5.

При розрахунку сумарної міцності декількох контурів захисту в формулу замість P_i включається P_{ki} – міцність кожного контуру, значення якої визначається за однією з формул тобто для контрольованих і неконтрольованих перепон, розрахунки повинні бути розділені і виконуватись для різних контурів, кожен з яких утворює окремий багаторівневий захист.

При $P_{ki} = 0$ даний контур не приймається в розрахунок. При $P_{ki} = 1$ решта контурів захисту є надлишковими. **Дана модель справедлива лише для контурів захисту, що перекривають одні й ті ж канали несанкціонованого доступу до одного й того самого предмету захисту.**

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

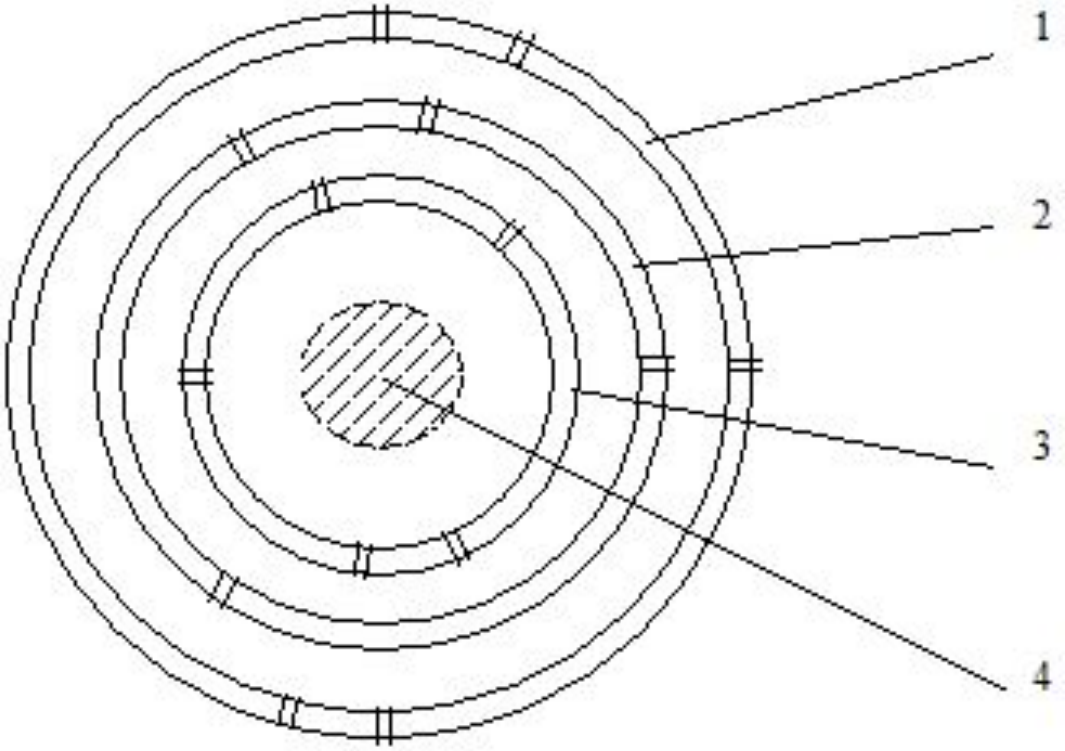


Рис. 16.5. Модель багаторівневого захисту:
1 - 1-й контур захисту; 2 - 2-й контур захисту;
3 - 3-й контур захисту; 4 - предмет захисту

Лекція 5
Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.4. Аналіз обчислювальної системи (ІС), як об’єкта захисту інформації

Аналіз існуючих в теперішній час систем обробки даних, а також АСУ показує, що з позиції захисту інформації об’єктом досліджень може бути вибрана обчислювальна система як самостійний об’єкт і як елемент територіально-розосередженої обчислювальної мережі чи великої АСУ. Не зупиняючись на конкретних реалізаціях обчислювальних систем з централізованою обробкою даних, що мають різні принципові для обробки інформації рішення, побудуємо її узагальнену модель, представлену на рис. 16.6, на якому інформація, що циркулює в обчислювальній системі, показана як дещо ціле, що підлягає захисту. Так як фізично інформація розміщується на апаратних і програмних засобах, останні представлені таким самим чином із зовнішньої сторони по відношенню до інформації.

Предмет захисту - інформація, що циркулює і зберігається в АСОД у вигляді даних, команд, повідомлень і т.п., що мають яку-небудь ціну для їх власника і потенційного порушника.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

При цьому за НСД приймаємо подію, що виявляється у спробі порушника здійснити несанкціоновані дії по відношенню до будь-якої її частини.

З позиції входу в систему і виходу з неї відзначимо найбільш характерні для більшості систем, готових до роботи, штатні засоби введення, виведення і зберігання інформації. До них відносяться наступні засоби:

-термінали користувачів;

-засоби відображення і документування інформації;

-засоби завантаження програмного забезпечення в систему;

-носії інформації: ОЗП, ПЗП, роздрукована інформація і т.д.

Усі перелічені засоби назвемо штатними каналами, по яким мають санкціонований доступ до інформації, що підлягає захисту, законні користувачі. Готовність системи до роботи означає, що система функціонує нормально, технологічні входи і органи управління в роботі не використовуються.

.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Відомо, що усю багатоманітність потенційних загроз інформації можна розділити на цілеспрямовані і випадкові. Природа ї точки їх прикладення різні.

Точки прикладення випадкових впливів розподілені по всій площі обчислювальної системи. Місце і час виникнення даних подій підкоряються законам випадкових чисел. Загроза випадкових впливів полягає у випадковому спотворенні чи формуванні невірних команд, повідомлень, адресів і т.д., що приводять до втрати, модифікації і витоку інформації, що підлягає захисту.

Відомі і засоби попередження, виявлення і блокування випадкових впливі. Це засоби підвищення достовірності інформації, що обробляється і передається. При цьому в якості засобів попередження, що скорочують імовірну кількість випадкових впливів, використовують схемні, схемотехнічні, алгоритмічні і інші заходи, що закладаються в проект обчислювальної системи. Вони направлені на усунення причин виникнення випадкових впливів, тобто зменшення імовірності їх появи.

Лекція 5
Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

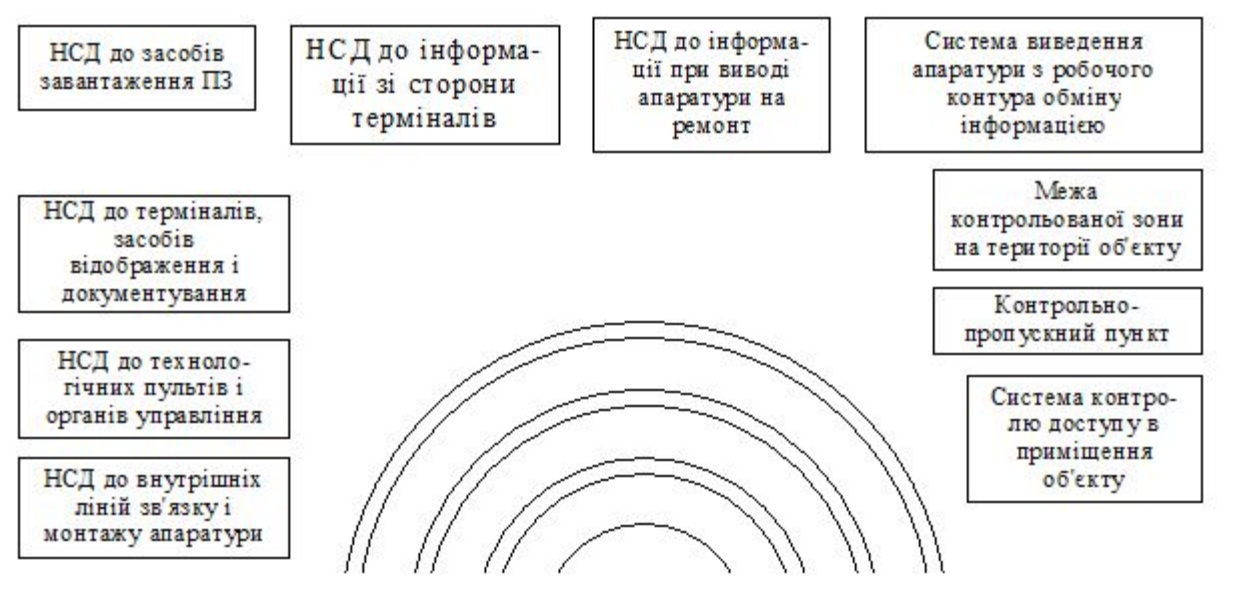


Рис 16.6 Модель обчислювальної системи з безпечною обробкою інформації

Лекція 5
Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В

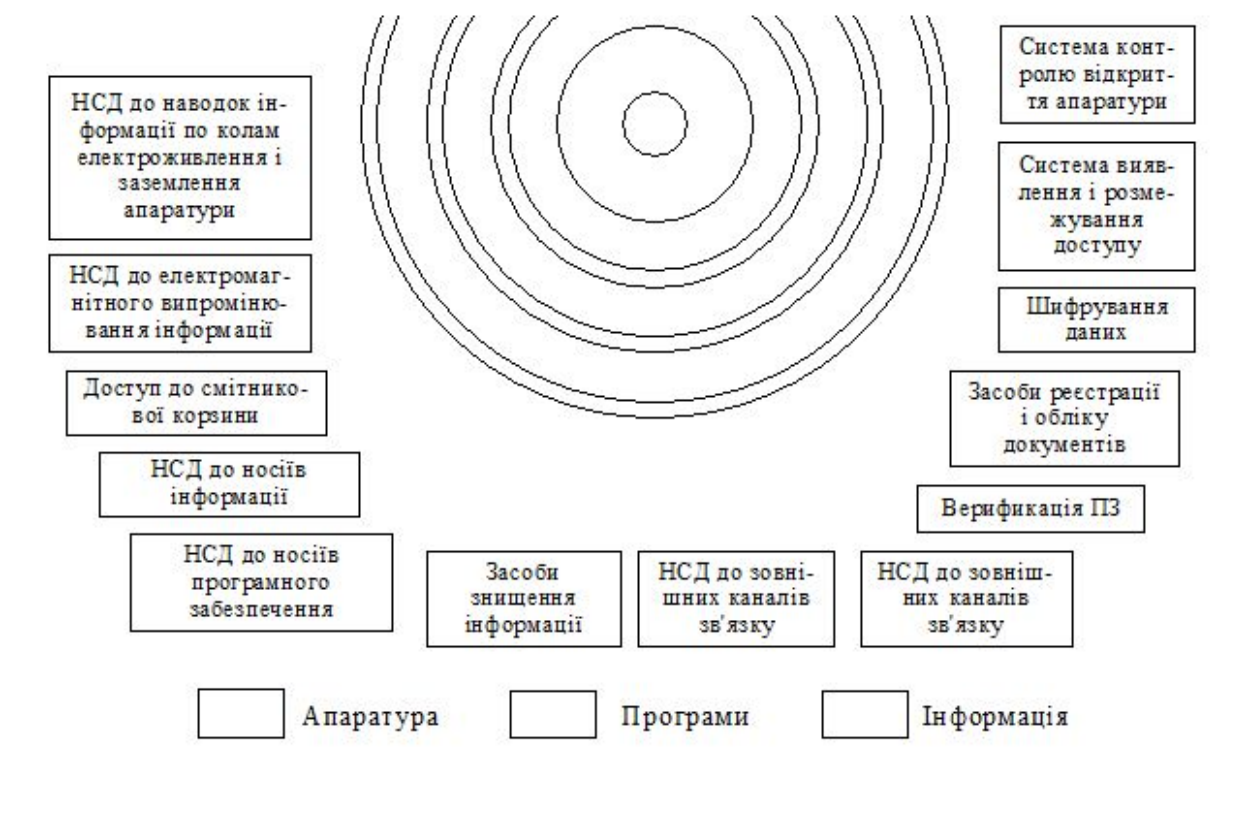


Рис 16.6 Модель обчислювальної системи з безпечною обробкою інформації (продовження)

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Оскільки після вказаних заходів імовірність їх появи все ж залишається значною, для виявлення і блокування випадкових впливів при експлуатації використовуються вбудовані в систему засоби функціонального контролю, якісними покчас виявлення і локалізації відмови;

достовірність контролю функціонування;

повнота контролю (охоплення обчислювальної системи);

час затримки і виявлення відмови.

Точки прикладення цілеспрямованих впливів пов’язані перш за все із входами в систему і виходами інформації з неї, тобто з периметром системи. Ці входи і виходи можуть бути законними і незаконними, тобто можливими каналами несанкціонованого доступу до інформації в обчислювальній системі можуть бути:

-всі перелічені вище штатні засоби при їх незаконному використанні;

-технологічні пульти і органи управління;

-внутрішній монтаж апаратури.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.5. Концептуальні основи для побудови захисту інформації від НСД в обчислювальній системі

Аналіз моделі обчислювальної системи, представленої на рис. 16.6., і моделей захисту, наведених в 16.3, дозволяє обчислювальну систему розглядати як об’єкт, в якому є деяка множина можливих каналів несанкціонованого доступу (МКНСД) до предмету захисту інформації.

Для побудови захисту інформації в даній системі на кожному МКНСД, а якщо можливо одразу на декількох необхідно установити відповідно перепону. Чим більша кількість можливих каналів НСД перекрита засобами захисту і вища імовірність їх неподолання потенційним порушником, тим вищий рівень безпеки інформації, що обробляється даною системою. Очевидно, що в реальній обчислювальній системі структура захисту буде мати багатоланковий і багаторівневий характер. Кількість МКНСД, що перекриваються, при цьому буде залежати від заданої кваліфікації порушника. Згідно запропонованій в розділі 16.3. класифікації можна встановити наступний розподіл МКНСД за класами.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

1-й клас - всі МКНСД, можливі в даній обчислювальній системі на поточний момент часу.

2-й клас - всі МКНСД, окрім ПЕВІН (побічне електромагнітне випромінювання і наводки) і машинних носіїв з залишками інформації, що підлягає захисту спеціальними криптографічними методами.

3-й клас - тільки наступні МКНСД:

-термінали користувачів;

-апаратура реєстрації, документування і відображення інформації;

-машинні і 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 наступні МКНСД:

-термінали користувачів;

-машинні і паперові документи;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

-засоби завантаження програмного забезпечення.

Аналіз можливих каналів НСД до інформації показує, що дані канали необхідно розділити на два види: контрольовані і неконтрольовані.

До контрольованих МКНСД обчислювальної системи можна віднести:

-термінали користувачів;

-засоби відображення і документування інформації;

-засоби завантаження програмного забезпечення;

-технологічні пульти і органи управління;

-внутрішній монтаж апаратури;

-побічні електромагнітні випромінювання;

-побічні наводки інформації в колах електроживлення і заземлення апаратури, допоміжних і сторонніх комунікаціях, розміщених поблизу апаратури обчислювальної системи.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

При цьому побічні випромінювання і наводки інформації, якщо говорити коректно, відносяться до цього виду каналів НСД у тому випадку, якщо рівень небезпечного сигналу, що несе інформацію, не виходить за межі контрольованої зони об’єкта обчислювальної системи і рівень цього сигналу періодично вимірюється в межах і за межами цієї зони.

У відповідності до моделі захисту (див. рис. 16.4) засоби захисту, що перекривають ці канали, утворюють віртуальний контрольований захисний контур.

До неконтрольованих каналів НСД до інформації обчислювальної системи слід віднести:

-машинні носії програмного забезпечення і інформації, що виносяться за межі обчислювальної системи;

-довготривалі запам’ятовуючі пристрої із залишками інформації, що виносяться за межі обчислювальної системи;

-зовнішні канали зв’язку;

-смітникова корзина.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Засоби захисту, що перекривають перелічені канали, утворюють віртуальний неконтрольований захисний контур.

Крім того, враховуючи множину користувачів, допущених до терміналів і інформації в середині обчислювальної системи, необхідне створення всебічної системи контролю і розмежування доступу. Розмежування доступу користувачів до інформації обчислювальної системи повинно виконуватись у відповідності з функціональними обов’язками і повноваженнями, що виконуються ними, і які можна змінити під час експлуатації системи.

Для того щоб забезпечити замикання контуру захисту із декількох різних за виконанням перепон, недостатньо тільки перекриття в обчислювальній системі всіх можливих каналів НСД. Необхідно ще забезпечити їх взаємодію між собою, тобто об’єднати їх в єдиний постійно діючий механізм. Цю задачу повинні виконувати централізовані засоби управління.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

На неконтрольованих МКНСД всі кола і тракти контролю апаратно, програмно і організаційно повинні сходитись на одному робочому місці служби безпеки інформації чи адміністратора обчислювальної системи. Останні варіант кращий для менш відповідальних систем при захисті інформації від порушника 3-го і 4-го класів. На неконтрольованих МКНСД централізоване управління повинно забезпечуватись аналогічним чином з тих самих робочих місь, але окремою функціональною задачею.

Наведені в розд. 16.3. моделі захисту, побудовані на основі прийнятої моделі поведінки потенційного порушника, що очікується, і придатні в принципі для використання в інших системах, окрім обчислювальних, для захисту іншого предмету, дають формальні представлення про механізм захисту і методи отримання його розрахункових характеристик в якісному і кількісному вираженні з гарантованими результатами.

Викладене дозволяє запропонувати за основу проектування і розроблення системи безпеки інформації в обчислювальній системі наступний порядок:

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

1) аналіз заданих вимог до АСОД на предмет визначення переліку, структури і динаміки вартості даних, що обробляються і підлягають захисту;
2) вибір моделі потенційного порушника;
3) виявлення в даній АСОД максимально можливої кількості каналів несанкціонованого доступу до інформації згідно вибраної моделі потенційного порушника;
4) аналіз виявлених МКНСД і вибір готових чи розробка нових засобів захисту, що спроможні їх перекрити з заданою міцністю;
5) якісна і кількісна оцінка міцності кожного із засобів захисту, що використовуються;
6) перевірка можливості адаптації засобів захисту в АСОД, що розробляється;
7) створення в АСОД, що розробляється, засобів централізованого контролю і управління;
8) кількісна і якісна оцінка міцності системи захисту інформації від НСД з окремими показниками по контрольованим і неконтрольованим МКНСД

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Аналіз запропонованого підходу до принципів побудови захисту говорить про ряд принципових властивостей предмету захисту, потенційних загроз і захисних перепон, які на відміну від прийнятих раніш концепцій доцільно враховувати при створенні ефективного захисту. Це наступні властивості:
інформація - об’єкт права власності, що підлягає захисту від НСД;
час життя інформації, що захищається;
-різні джерела, місце і час прикладення випадкових і цілеспрямованих НСД;
-наявність достатньо простої моделі потенційного порушника;
-ступень охоплення обчислювальної системи функціональним контролем і засобами підвищення достовірності інформації, яка визначає імовірність появи випадкових НСД;
-можливі канали НСД до інформації;
-ступень замикання перепони навколо предмету захисту, що визначає імовірність її обходу порушником;
-ділення можливих каналів НСД на контрольовані і неконтрольовані;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

-залежність міцності перепони, що немає властивості контролю НСД, від співвідношення часу життя інформації і часу подолання перепони порушником, що очікується;
-залежність міцності перепони, що має властивість контролю НСД, від властивості перепони до своєчасного виявлення і блокування спроб НСД;
-залежність рівня міцності захисту інформації в АСОД в цілому від рівня міцності найслабшої ланки;
-можливість створення системи захисту інформації у вигляді єдиного цілого і реально діючого механізму.

Основна тактика і стратегія захисту інформації від НСД в обчислювальній системі полягає у виконанні наступних задач:
-попередженні і контролі спроб НСД;
-своєчасному виявленні, визначенні місця і блокуванні несанкціонованих дій;
-реєстрації і документуванні подій;
-установленні і усуненні причин НСД;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Попередження і контроль НСД полягає в наступному:

1. Для захисту від випадкового НСД використання засобів функціонального контролю технічних засобів АСОД і засобів підвищення достовірності інформації.
2. Для захисту від цілеспрямованих НСД створення в АСОД замкненого контуру захисту, що складається із системи перепон, які перекривають максимально можливу кількість каналів НСД і мають таку міцність, затрати часу на подолання якої більші часу життя інформації, що захищається, чи більші часу виявлення і блокування НСД до неї.

Задачею захисту є створення в АСОД єдиної системи взаємопов’язаних перепон, які забезпечують надійне перекриття можливих каналів несанкціонованого доступу від впливів, направлених на втрату, модифікацію і витік інформації, тобто на безпеку інформації. Настання однієї з цих подій, не передбачених штатним режимом роботи АСОД, розглядається як факт здійснення НСД.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Втрата полягає у стиранні, спотворенні, знищенні чи крадіжці інформації, що знаходиться в процесі обробки чи зберігання в АСОД. Небезпека її полягає у безповоротній втраті цінної інформації.

Модифікація полягає у зміні інформації на хибну, яка коректна по формі і вмісту, але має інший зміст. Нав’язування хибної інформації при відсутності законної і недоведення законної інформації до одержувача можна також рахувати її модифікацією. Прикладом модифікації може бути зміна дати документу, кількість сировини і матеріалів, суми грошей і т.д. Небезпека модифікації полягає у можливості організації витоку секретної чи (і) передачі хибної інформації в подальшу обробку і використання.

Втрата інформації полягає в несанкціонованому ознайомленні сторонньою особою з секретною інформацією. Небезпека витоку інформації полягає в розголошенні приватної, комерційної, службової, військової чи державної таємниці із усіма наслідками, що випливають звідси.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

З викладеного також слідує, що в забезпечення безпеки входить не тільки захист секретної, але частини несекретної інформації. Прикладом такого виду інформації і необхідності її захисту від НСД є інформація в ЛОМ в Агентстві по охороні оточуючого середовища.

На основі викладеного можна дати наступне визначення автоматизованої системи з безпечною обробкою даних.

Автоматизована система обробки даних забезпечує їх безпеку, якщо в ній передбачена централізована система керованих і взаємопов’язаних перепон, що перекривають з гарантованою міцністю задану у відповідності з моделлю потенційного порушника кількість можливих каналів несанкціонованого доступу і впливів, направлених на втрату чи модифікацію інформації, а також несанкціоноване ознайомлення з нею сторонніх осіб.

Запропонований підхід відповідає змісту захисту і дозволяє побудувати на шляху порушника чітку систему рівно-міцних і взаємопов’язаних перепон з можливістю обгрунтованого визначення кількісних і якісних параметрів на основі окремих засобів захисту.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

16.6. Концептуальні основи для проектування захисту інформації від НСД в обчислювальній мережі і АСУ

Узагальнені моделі обчислювальних мереж як об’єктів захисту інформації, що пропонувались до сих пір, з одного боку, - надто глибоко віддзеркалювали її структуру, а з другої - не повністю враховували системні зв’язки і відношення між її елементами, так як за основу моделі брався неповний фрагмент архітектури мережі. Акцент знову робився на захисті ресурсів мережі (вузлів обробки інформації), а не на самій інформації, а також на її децентралізованій обробці. Напевно, з цієї самої причини в опублікованих в останній час роботах майже забуті АСУ, які ще живуть, будуть жити і розвиватись. Між іншим зауважимо, що обчислювальну мережу з позицій управління також можна назвати АСУ, так як в неї є свої централізовані засоби управління її функціонуванням і обробкою інформації. Отже, повинні бути і засоби управління безпекою інформації. Відрізняють мережі і АСУ тільки системні відношення між їх керованими ланками.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

В АСУ може бути багатоступінчата ієрархічна структура, а в мережі - завжди двоступінчата. Тому в якості об’єкта дослідження пропонується розглянути деяку узагальнену модель структури АСУ, наведену на рис. 16.1б (розд. 16.2.).

На рисунку АСУ представлена як сукупність КЗА, з’єднаних між собою каналами зв’язку. При цьому під КЗА розуміється будь-яка територіально-зосереджена АСОД, побудована на базі комплексу технічних засобів, об’єднаних загальним програмним забезпеченням і виконанням однієї з декількох спільних задач. Згідно своєї ролі в АСУ і в мережі передачі даних КЗА в тій чи іншій структурі зв’язані певними системними зв’язками.

Одна група КЗА, наприклад вузли комутації повідомлень, разом з другою групою КЗА (апаратурою передачі даних) утворюють мережу передачі даних, друга група КЗА (обчислювальні комплекси, системи, абонентські пункти і т.д.) разом з цією мережею утворюють АСУ. В кожної з названих структур є свої задачі і межі, які повинні забезпечуватись засобами захисту і контролюватись відповідними засобами управління.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Якщо таким власником є держава, то повинна бути особа, яка несе таку відповідальність. В цьому аспекті створення для всіх користувачів єдиного обчислювального середовища є безнадійною задачею і використання терміну захищене обчислювальне середовище виправдане тільки у філософському змісті.

В інтересах виконання системних задач по обробці інформації АСУ (мережа) містить наступні засоби управління:

-засоби управління складом і конфігурацією АСУ (мережі);
-засоби управління структурно-адресними таблицями;
-засоби управління функціональним контролем АСУ (мережі);
-засоби управління функціонуванням АСУ (мережі).

Перелічені засоби розташовуються на одному з елементів АСУ (мережі), що керує КЗА АСУ (мережі). Окрім вказаних засобів АСУ містить засоби взаємодії її складових частин (КЗА) між собою, які визначають характер системних зв’язків. Ці зв’язки пов’язані з виконанням основних задач АСУ.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Наведена на рис. 16.1б структура АСУ дозволяє визначити всього два види можливих каналів НСД до інформації АСУ (мережі): КЗА і канали зв’язку. Концепція безпеки інформації на рівні КЗА була розглянута вище в розд. 16.5. Отже, залишається розглянути тільки концепцію захисту інформації в каналах зв’язку.

Приймаючи до уваги, що інформація в АСУ (в мережі) постійно поновлюється, а також і те, що на каналах зв’язку на відміну від елементів АСУ (мережі) порушник нічим не ризикує, особливо при пасивному перехопленні інформації, міцність захисту тут повинна бути особливо високою. Від активного втручання порушника в процес обміну інформацією між елементами АСУ (мережі) повинна бути використана система виявлення і блокування НСД. Але й при цьому ризик порушника як і раніш невисокий, так як у нього у цьому випадку з причини складності визначення його місця перебування залишається достатньо часу на те, щоби відключитись і знищити свої сліди. Тому в якості вихідної моделі потенційного порушника слід вибрати порушника високої кваліфікації

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Такий підхід допоможе захиститись також і від порушників, які є законними користувачами даної АСУ (мережі). Крім того, це дозволить захистити системні зв’язки між елементами АСУ (мережі).

Оскільки фізичні канали зв’язку в мережі захистити не представляється можливим, доцільно будувати захист інформації і супроводжуючих її службових ознак на основі спеціальних криптографічних перетворень, тобто на основі самої інформації, а не на ресурсах АСУ (мережі). Дана кодограма, як правило, містить адрес одержувача, заголовок, інформацію відправляча, кінцевик, адрес відправляча, вихідний номер і час відправлення. В пакетному режимі добавляється ще і номер пакету, оскільки повідомлення розбивається на пакети, які на об’єкті-одержувачі повинні бути зібрані в одне повідомлення, щоб воно набуло початкового вигляду. Для синхронізації прийому і обробки кодограми в неї включають ознаки кадру.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Кінцевик містить перевірочне поле, що служить для корекції і виправлення помилок (при завадостійкому кодуванні), внесених каналом. Для забезпечення передач блоків даних від станції, що передає, до приймальної кодограма містить ознаки маршруту. Всі ці і інші складові кодограми формуються на основі відомої семирівневої моделі протоколів взаємодії відкритих систем JSO/OSI/

Аналіз проведених досліджень в області безпеки інформації в обчислювальних мережах дозволяє взяти за основу наступні вимоги, які повинні бути кінцевою метою при створенні засобів її захисту.

Після того як з’єднання між двома абонентами обчислювальної мережі встановлене, необхідно забезпечити чотири умови:

а) одержувач повідомлення повинен бути впевненим в правдивості джерела даних;

б) одержувач повинен бути впевненим в правдивості отриманих даних;

в) відправляч повинен бути впевненим в доставці даних одержувачу;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

г) відправляч повинен бути впевненим у правдивості доставлених одержувачу даних.

При цьому мається на увазі, що виконання цих умов включає захист від наступних активних втручань порушника:

вплив на потік повідомлень: зміна, вилучення, затримка, переупорядкування, дублювання регулярних і подання хибних повідомлень;

протидія передачі повідомлень;

реалізація неправильних з’єднань.

Однак вони не захищають від пасивних втручань:

-читання змісту повідомлень;

-аналізу трафіку і ідентифікаторів абонентів мережі.

Крім того необхідно відмітити важливі моменти: одержувач не повинен приймати всі повідомлення підряд, хоча б вони були правдивими і від дійсних джерел, а відправних повідомлення повинен бути впевненим, що одержувач правильно відреагує на нього.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Іншими словами, і відправник, і одержувач повинні в даній мережі (АСУ) мати повноваження на обмін один з одним. Це необхідно не для обмеження їх свободи, а для забезпечення довір’я один до одного і довір’я їх до автоматизованої системи, що є святим обов’язком будь-якої обчислювальної мережі і АСУ з точки зору юридичного права незалежно від того, дружать вони чи не дружать між собою. Якщо користувач звертається у віддалену базу даних, юридичну відповідальність, з однієї сторони, несе користувач, з другої - власник даної АСОД.

Таким чином, для повноти постановки задачі до вказаних чотирьох умов необхідне доповнення ще чотирьох:

д) відправляч і одержувач повинні бути впевнені в тому, що з доставленої інформації в повідомленні ніхто, крім них, не ознайомився;

е) відправляч і одержувач повинні бути впевнені, що нікому, крім них і спеціального посередника, факт передачі повідомлення між ними не відомий;

ж) одержувач повинен бути впевненим, що відправляч - це та особа, за яку себе видає;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

з) відправляч повинен бути впевненим, що одержувач - це особа, яка цому необхідна для передачі повідомлення.

Дані вимоги (а - з) розраховані на захист від кваліфікованого порушника-професіонала за кваліфікацією, що наведена в розд. 16.3.

Для визначення основних принципів вирішення цієї задачі розглянемо згадану вище уніфіковану кодограму, яка є носієм цієї інформації і, отже, предметом захисту.

Виходимо з того, що порушнику доступна вся кодограма, включаючи службові ознаки, а також з того, що єдиним методом захисту з цієї причини може бути вибраний метод криптографічних перетворень.

Один з методів повинен бути таким, щоб в кодограмі зберігались деякі адреси і службові ознаки у відкритому вигляді, оскільки всю кодограму перетворювати недоцільно з причини неможливості її подальшої обробки. Таким методом може бути використання механізму формування цифрового (електронного) підпису на базі несиметричних алгоритмів шифрування.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Крім того окремі частини кодограми формуються на різних етапах її обробки різними пристроями і вузлами мережі; частина цієї інформації належить їй, а друга частина - її абонентам. Це визначає, кому належать і хто має ключі шифрування тієї чи іншої частини кодограми: АСУ чи СПД.

Шифрування частин кодограми зручно виконувати одночасно з формуванням відповідних ознак обробки повідомлення і його самого при реалізації протоколів семирівневої моделі взаємодії відкритих систем JSO/OSI.

Для того щоб забезпечити можливість контролю і розмежування доступу, необхідно для всіх учасників обміну інформацією, окрім умовних номерів, присвоїти змінні ідентифікатори у вигляді паролів, які можуть передаватись у відкритому вигляді і відповідність яких буде забезпечуватись механізмом цифрового підпису. Тим абонентам, яким присвоєні відповідні повноваження, повинні бути надані відповідні значення паролів і закритих ключів шифрування.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Таким чином, розрахунок безпеки інформації в каналах зв’язку можна проводити на основі групи показників механізмів шифрування, що використовується для кожної складової кодограми. Стійкість, чи міцність, захисного механізму визначається стійкістю до підбору використаного секретного ключа в кількості часу, що використовується порушником на цю роботу. Якщо вона складає величину, що перевищує час життя інформації, що захищається, то міцність чи імовірність цієї перепони дорівнює 1.

При цьому звернемо увагу на існуючу різницю в часі життя самого повідомлення і його службових частин. Саме повідомлення в залежності від призначення АСОД може зберігати цінність десятки років, а його службові частини - не більше десяток хвилин (час доведення повідомлення до адресату). Це дозволяє істотно збільшити швидкодію шифрування і, можливо, навіть спростить його для службових частин. Такий великий набір процедур може викликати сумнів в розробників з приводу реальності втілення цієї ідеї через можливість збільшення часу обробки кодограми.

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

Однак навіть якщо це станеться, підвищення безпеки інформації вартує цього. При реалізації системи контролю і розмежування доступу в АСУ (СПД) необхідно також організувати систему збору з КЗА сигналів незбігання кодів паролів, систему управління і розподілення ключів шифрування інформації і організаційні заходи по безпеці інформації.

Викладене дозволяє запропонувати наступну групу засобів для забезпечення безпеки інформації, що обробляється в каналах зв’язку, орієнтованих відповідно на виконання наведених вище восьми умов:

а) засоби формування цифрового підпису повідомлення;

б) засоби шифрування даних, що передаються;

в) засоби забезпечення цифрового підпису службових ознак інформації, що передається, включаючи адреси і маршрути повідомлень, а також отримані відправником і посередником квитанції від одержувача;

г) всі перелічені в п. а, б і в засоби;

д) засоби п. б;

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

е) введення в СПД маскуючих потоків повідомлень при відсутності активності в обміні інформацією;

ж) присвоєння всім учасникам обміну повідомленнями змінних ідентифікаторів і створення в АСУ і СПД системи контрою і розмежування доступу із захистом цифровим підписом паролів від підміни їх порушником;

з) засоби ті ж самі, що і в п. ж.

Показник міцності перелічених засобів захисту і буде в результаті визначати безпеку інформації в каналах зв’язку. Враховуючи високу вартість каналів зв’язку і небезпеку втручання порушника-професіонала, розрахунок міцності вказаних засобів (оскільки це тепер технічно можливо) пропонується проводити тільки при забезпеченні умови, коли очікуваний час, що витрачається порушником, повинен бути більше часу життя інформації, що захищається. Це доцільно виконувати завжди незалежно від заданого класу потенційного порушника

Глава 16.

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АСОД

В деяких мережах і АСУ не потребується захист трафіку і захист від витоку інформації. Тому автором пропонується ввести для каналів зв’язку наступну класифікацію вимог по класам потенційного порушника:

1-й клас - всі вимоги;

2-й клас - всі, крім вимоги е;

3-й клас - всі, крім вимог б, г, д і е.

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

В процесі підготовки до початку робіт по проектуванню АСОД при узгодженні технічного завдання в принципі вже відомі попереднє розподілення, місце зосередження, характер, ступінь важливості і секретності інформації, що підлягає обробці. Таким чином визначається необхідність в розробленні системи захисту інформації і відповідних вимог до неї, які обов’язково повинні бути наведені в технічному завданні на систему. Звідси випливає основна вимога до порядку проведення проектування, що полягає в необхідності паралельного проектування системи захисту інформації і проектування системи управління і обробки даних, починаючи з моменту вироблення загального задуму побудови АСОД. Створенню системи захисту інформації, вбудованої в автоматизовану систему, властиві всі етапи: розробка технічної пропозиції, ескізного і технічного проектів, випуск робочої документації. Виготовлення, випробовування і здача системи замовнику.

Лекція 5
Гарантоздатність автоматизованих систем

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Невиконання цього принципу, накладання чи вбудова засобів захисту у вже готову систему, може привести до низької ефективності захисту, неможливості створення цільної системи захисту, зниженню продуктивності і швидкодії обчислювальних засобів, а також до великих витрат, ніж якщо б система захисту розроблялась і реалізувалась паралельно основним задачам.

При паралельному проектуванні розробниками системи захисту інформації (СЗІ) проводиться аналіз циркуляції і місць зосередження інформації в проекті АСОД, визначаються найбільш уразливі для НСД точки і своєчасно пропонуються взаємоприйнятні технічні рішення по скороченню їх кількості шляхом зміни принципової схеми АСОД, що дозволить забезпечити простоту, надійність і економічність реалізації захисту з достатньою ефективністю. Крім того, паралельне проектування необхідне в силу вбудованого характеру більшої частини технічних засобів захисту.

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Функціонування механізму захисту повинно плануватись і забезпечуватись поряд з плануванням і забезпеченням процесів автоматизованої обробки інформації, що важливо для визначення ступеня впливу СЗІ на основні імовірнісно-часові характеристики АСОД, які, як правило, змінюються в сторону погіршення. Все це - плата за набуття нової і необхідної якості, яка інколи є причиною зневажливого відношення деяких розробників і замовників АСОД до захисту. Однак за таку недальновидність їм доводиться розплачуватись потім неспівмірно більш дорогою ціною. Не виконавши цю задачу, вони позбавили власника АСОД гарантій на власність його інформації, що циркулює в ній.

При розробці технічного завдання і подальшого проектування АСОД слід пам’ятати, що створення системи захисту інформації - задача не другорядна, оскільки невиконання її може бути причиною недосягнення мети, що ставиться перед АСОД, втрати довір’я до неї, а в деяких випадках витоку і модифікації інформації.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Технічне завдання на проектування АСОД повинно містити перелік відомостей і характеристик, що підлягають захисту, можливі шляхи циркуляції і місця їх зосередження, а також спеціальні вимоги до системи захисту інформації. Якщо це АСУ чи обчислювальна мережа, то повинна дотримуватись ієрархія вимог до СЗІ (системи захисту інформації). Вони повинні входити:

-в загальне технічне завдання на АСУ чи мережу в цілому;

-в часткове технічне завдання на функціональні підсистеми управління, на окремі автоматизовані ланки, об’єкти, комплекси, технічні засоби;

-в технічне завдання на спряження зовнішніх систем;

-в технічне завдання на загальне програмне забезпечення окремих ЕОМ і обчислювальних комплексів, на спеціальне програмне забезпечення об’єктів - елементів обчислювальної мережі чи АСУ.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Перше знайомство з АСОД, що розробляється, повинно закінчитись рекомендаціями по скороченню виявлених каналів доступу шляхом її принципової зміни без втрат для виконання її основних задач.

Аналіз найважливіших задач організації і формування функцій, що задовольняють цілям управління, носить звичайно ітеративний характер, що забезпечую послідовне уточнення задач і функцій, узгодження їх на всіх рівнях і ступенях АСУ і зведення в єдину функціональну схему. Це означає, що проведені на деякому етапі проектування технічні рішення, що накладаються системою захисту на основні задачі АСУ, повинні перевірятися за ступенем їх впливу на рішення основних процесів і навпаки: після прийняття рішення по зміні основних процесів управління і складу технічних засобів повинна перевірятись їх відповідність рішенням по захисту інформації, які при необхідності повинні коректуватись чи зберігатись, якщо коректування зменшує міцність захисту.

Лекція 5

Гарантоздатність автоматизованих систем

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Важливу роль грає простота системи захисту. Вона повинна бети простою настільки, наскільки дозволяють вимоги до її ефективності. Простота захисту підвищує його надійність, економічність, зменшує його вплив на імовірнісно-часові характеристики АСУ, створює зручності у спілкуванні з ним. При незручних засобах захисту користувач буде намагатись знайти шляхи його обходу, відключити його механізм, що зробить захист таким , що немає змісту і непотрібним.

При проектуванні захисту, як і у звичайних розробках, цілком розумно використання уніфікованих чи стандартних засобів захисту. Однак, бажано, щоб вказані засоби при використанні в АСОД, що проектується, набуло індивідуальної властивості захисту, які б не були відомі потенційному порушнику.

Дані по захисту інформації в АСОД, що проектується, повинні міститись в окремих документах і засекречуватись.

Лекція 5
Гарантоздатність автоматизованих систем

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Ознайомлення досвідчених і кваліфікованих спеціалістів з уразливими точками проекту на предмет його доробки можна здійснити шляхом організації контрольованого доступу їх до секретного проекту. У цьому випадку по крайні мірі будуть відомі особи, які ознайомлені з проектом. Таким чином скорочується число осіб - потенційних порушників, а особи, ознайомлені з проектом, несуть відповідальність перед законом, що, як відомо, є стримуючим фактором для потенційного порушника.

В процесі проектування і випробовування рекомендується по можливості використовувати вихідні дані, що відрізняються від дійсних, але такі, що дозволяють при наступному завантаженні системи дійсними даними не проводити доробки. Завантаження дійсних даних повинно проводитись тільки після перевірки функціонування системи захисту інформації в даній АСОД.

Лекція 5

Гарантоздатність автоматизованих систем

Національний університет “Львівська політехніка”
Кафедра захисту інформації

Глава 17.

ОСНОВНІ ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБРОБКИ ДАНИХ

Враховуючи те, що система захисту в АСОД передбачає, окрім апаратно-програмних засобів, використання в якості перепони і організаційних заходів, що виконуються людиною - найбільш слабою ланкою захисту, необхідно прагнути до максимальної автоматизації її функцій і скороченні долі її участі в захисті.

Для того щоб спроектована система захисту набула життя, необхідно також, щоб технічні засоби захисту по можливості не погіршували імовірнісно-часові характеристики АСОД: швидкодію, продуктивність і інші. При проектуванні необхідно знайти розумне співвідношення в задоволенні одних і других вимог.

Лекція 5

Гарантоздатність автоматизованих систем