Тема 10

ІНФОРМАЦІЙНА БЕЗПЕКА В ІСМ

Комерційна інформація – це

будь-яка інформація, яка зберігається і та обробляється в комп'ютері, є чиєюсь власністю і становить інтерес для певного кола осіб.

Комерційна таємниця

І. У сфері виробництва:

- структура кадрів;
- характер виробництва;
- відомості про виробничі можливості підприємства;
- дані про резерви сировини і плановані закупки;
- відомості про використовувані і перспективні технології;
- плани розвитку підприємства.

Комерційна таємниця

III. У бізнесі:

- дані контрактів та угод, які виконуються організацією;
- дані про перспективні проекти та угоди, бізнес-плани;
- дані про персонал;
- дані про використовувані ноу-хау;
- дані про поточну діяльність організації;
- дані обліку (оперативного, бухгалтерського тощо);
- дані, необхідні для функціональної діяльності всіх підрозділів організації.

Безпека інформації – це

створення таких умов зберігання, оброблення і передавання інформації, за яких вірогідність її витікання, модифікації або руйнування задовольняє задані вимоги.

Проблеми захисту інформації

- відмова мережі (24%);
- помилки програмного забезпечення (14%);
- комп’ютерний вірус (12%);
- зіпсованість комп’ютера (11%);
- викрадення даних (7%);
- саботаж (5%);
- несанкціоноване проникнення в мережу (4%);
- інші (23%).

Об'єкти, на яких має гарантуватися інформаційна безпека

- споруди, приміщення і території, на яких розташовані автоматизовані ІС і де можуть проводитись переговори і обмін конфіденційною інформацією;
- технічні засоби автоматизованих ІС - комп'ютерні обладнання, обладнання локальних мереж, кабельна система, телекомунікаційне обладнання;
- програмні засоби автоматизованих ІС;
- інформація, що зберігається і обробляється у автоматизованій ІС;
- автономні носії інформації (компакт-диски, дискети тощо);
- співробітники організації, які працюють з автоматизованою ІС і є носіями конфіденційної інформації та комерційної таємниці.

Основні види заходів захисту інформації в ІС

№ з/п	Заходи	Зміст
1	Органі заційні	Охоплюють порядок роботи з конфіденційною інформацією: регламентація доступу у приміщення і безпосередньо до обчислювальної техніки, додержання певних норм і протоколів і відповідальність за їх порушення.
2	Норма тивні	Регламентують правила використання та оброблення інформації обмеженого доступу та встановлюються міри відповідальності за їхнє порушення. Визначаються законодавчими актами, які регламентують правила користування, опрацювання та передачі інформації обмеженого доступу та встановлюють міру відповідальності за порушення цих правил. В Україні введена кримінальна відповідальність за незаконне втручання в роботу комп'ютерів чи поширення комп'ютерних вірусів, яке призводить до спотворення, зникнення або блокування доступу до інформації чи носіїв.

Основні види заходів захисту інформації в ІС

№ з/п	Заходи	Зміст
3	Фізичні	Охорона, сигналізація, створення екранованих приміщень для захисту від витікання інформації по каналах випромінювання, перевірка апаратури, що поставляється, на відповідність її специфікаціям та відсутність апаратних “жучків”.
4	Апаратно-програмні засоби	Основними засобами захисту інформації під час використання технічних засобів є: •пошук закладних (підслуховуючих/записуючих) пристроїв; •забезпечення прихованості передавання інформації по телефонно-телеграфних каналах їхнім шифруванням; •спеціальний захист апаратури від випромінювань за допомогою захисних блоків; •створення штучних перешкод щодо перехоплення електричних або акустичних сигналів. •реалізують технічні і програмні (наприклад, криптографічні) методи захисту. Серед головних вимог до збереження конфіденційної інформації є конфіденційність, цілісність, аутентифікація, авторизація, гарантії і зберігання таємниці. Стрижнем захисту є криптографічні засоби, які використовують для таких цілей: •шифрування інформації для захисту як від несанкціонованого доступу з боку користувача-порушника; •контроль цілісності даних та програм з метою виявлення випадкових та навмисних спотворень;. •аутентифікація документів з метою перевірки цілісності їх вмісту та підтвердження істинності авторства на основі цифрового підпису.

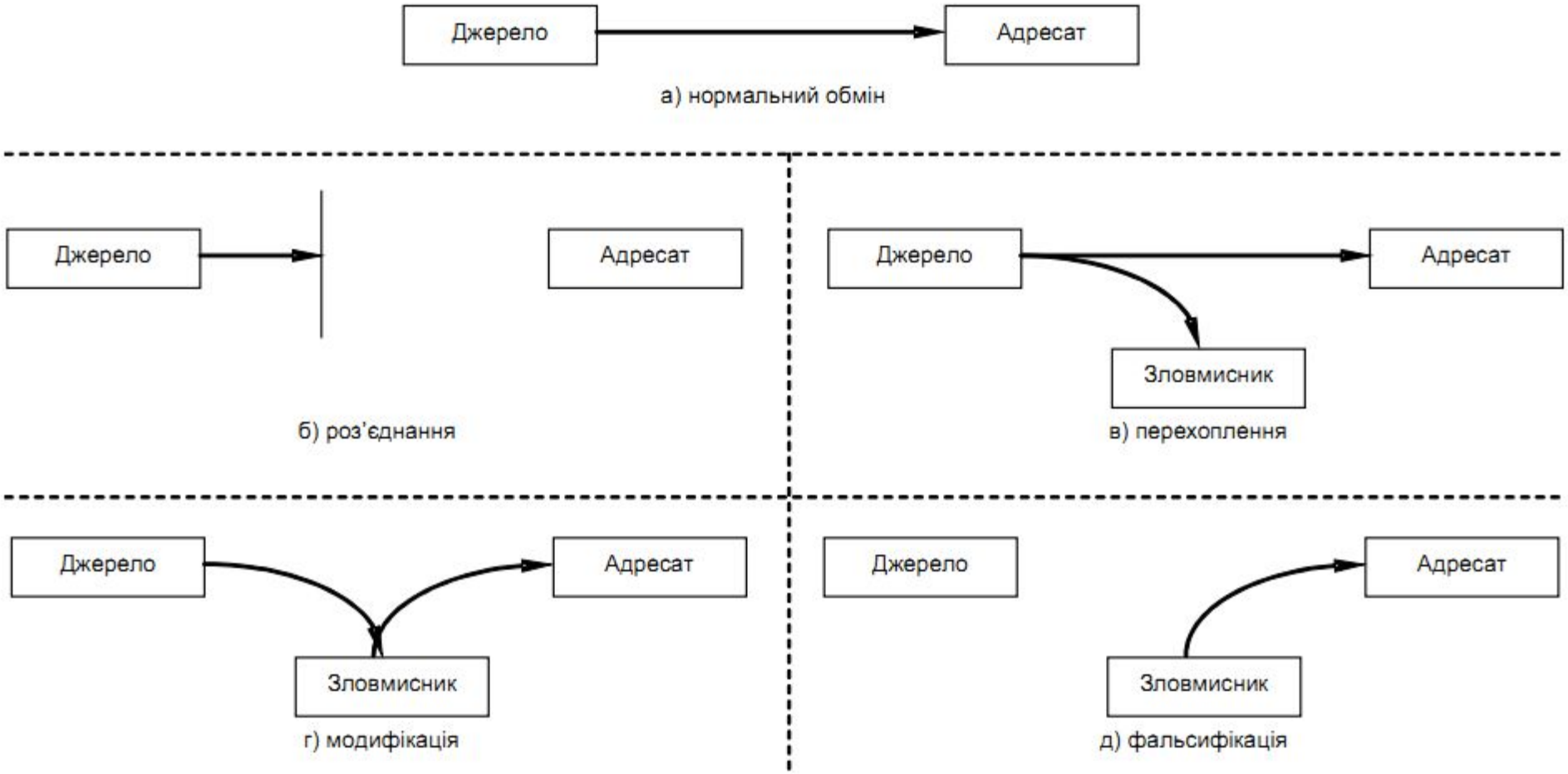
Вимоги до захисту інформації

- економічність;
- недопущення ускладнення управління в зв'язку з її використанням;
- комплексність;
- одночасність створення ІСМ і системи захисту інформації в ній;
- ієрархічність.

Принципи побудови системи захисту інформації в ІС

№ з/п	Принцип	Зміст
1	Комплексний підхід до побудови системи захисту при провідній ролі організаційних заходів	Означає оптимальне поєднання програмних апаратних засобів і організаційних заходів захисту
2	Розділення і мінімізація повноважень по доступу до оброблюваної інформації і процедур обробки	Надання користувачам мінімуму строго визначених повноважень, достатніх для успішного виконання ними своїх службових обов'язків, з погляду автоматизованої обробки доступною їм конфіденційній інформації
3	Повнота контролю і реєстрації спроб несанкціонованого доступу	Точне встановлення ідентичності кожного користувача і протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІС без її попередньої реєстрації.
4	Забезпечення надійності системи захисту	Підтримання заданого рівня безпеки при виникненні збоїв, відмов, навмисних дій порушника або ненавмисних помилок користувачів і обслуговуючого персоналу.

Схеми механізмів порушень безпеки даних



Види загроз безпеці інформації та методи її захисту

Загроза	Рішення	Дія	Технологія
Дані навмисно перехоплюються, читаються або змінюються	Шифрування	Кодування даних, що перешкоджає їх прочитанню або перекручуванню	Симетричне або асиметричне шифрування
Користувачі ідентифікують себе неправильно (з метою шахрайства)	Аутентифікація	Перевірка істинності відправника й одержувача	Цифрові підписи
Користувач одержує несанкціонований доступ з однієї мережі в іншу	Брандмауер	Фільтрація трафіка, що надходить у мережу або на сервер	Брандмауери, віртуальні приватні мережі

Класи безпеки ІС

Рівень	Клас	Характеристика ІС
Високий клас	A_1: верифікація	ІС задовольняють вимогам класу B_3 та додатково для перевірки специфікацій застосовуються методи формальної верифікації — аналізу специфікацій системи щодо неповноти або суперечності, що може привести до появи проривів у безпеці.
Проміжний клас	B_1: захист мітками	ІС з цілком контрольованим доступом, в якій всі суб'єкти і об'єкти забезпечуються мітками (або рівнями) конфіденційності і рішення на доступ суб'єкта до об'єкта приймається за заздалегідь визначеним правилом на основі зіставлення інформації обох міток.
	B_2: структурований захист	Додатково до вимог класу B_1 вимагається наявність добре визначеної і задокументованої формальної моделі політики безпеки, яка потребує дії вибіркового і повноважного керування доступом до всіх об'єктів системи. Вводяться вимоги керування інформаційними потоками відповідно до політики безпеки.
	B_3: сфери безпеки.	У ІС визначаються сфери безпеки, які будуються за ієрархічною структурою і захищені одна від одної за допомогою спеціальних механізмів. Усі взаємодії суб'єктів з об'єктами жорстко контролюються спеціальним монітором. Система контролю сповіщає адміністратора безпеки і користувача про порушення безпеки.
Низький клас	C_1: вибірковий захист	ІС, що задовольняють вимогам вибіркового керування доступом, забезпечуючи розділення користувачів і даних. Для кожного об'єкта і суб'єкта задається перелік допустимих типів доступу (читання, запис, друкування тощо) суб'єкта до об'єкта. Обов'язкова ідентифікація і аутентифікація суб'єкта доступу, а також підтримка з боку обладнання.
	C_2: керований доступ	ІС типу C_1, в яких додаються вимоги унікальної ідентифікації суб'єкта доступу, захисту з умовчання і реєстрації подій. Унікальна ідентифікація означає, що будь-який користувач системи повинен мати унікальне ім'я. Захист за замовчуванням передбачає призначення повноважень доступу користувачам за принципом “все, що не дозволено, заборонено”. Тобто всі ті ресурси, що явно не дозволені користувачеві, розглядаються як недоступні. У цих ІС обов'язкове ведення системного журналу, в якому відмічаються події, пов'язані з безпекою системи.

Класи безпеки захисту інформації

Клас	Призначення
Перший	означає наявність розвинутої служби безпеки
Другий	включає повний набір механізмів захисту на декількох рівнях
Третій	захист при багатьох суб'єктах і об'єктах, допущених до інформації
Четвертий	захист електронних платежів
П'ятий	захист розподілених інформаційних мереж
Шостий	захист локальних інформаційних мереж
Сьомий	мінімальні вимоги до захищеності

Методи боротьби з дезінформацією

- повторювати особливо важливу інформацію в різних формах, через різні інформаційні потоки з метою досягнення певної насиченості організації цією інформацією;
- підтверджувати правильність попередніх повідомлень, порівнюючи їх з інформацією, отриманою з інших джерел;
- зменшувати кількість посередників у потоках інформації за допомогою безпосередніх контактів керівників з працівниками;
- чітко визначати інформаційні потоки, які доцільно спрямовувати (що сприймати повністю, а що - лише вибірково; якими джерелами інформації користуватись