МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ТЕМА 1: СТАН та ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНО-ВАЖЛИВИХ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ ПРОВІДНИХ КРАЇН СВІТУ і УКРАЇНИ

Лекція 3: «Загрози та головні уразливості критично-важливих об'єктів інфраструктури»

***МЕТА ЛЕКЦІЇ*:**
визначення суті понять "загроза" та "уразливість" КВОІ

Викладач:

Передумови появи, природа походження та джерела загроз

Загроза безпеці - явища, дії, умови та фактори, що являють собою небезпеку для різних категорій управління: інформації, інфраструктури, суб'єктв, об'єктів та порядку управління. Небезпека полягає у можливості порушення властивостей однієї або декількох вказаних категорій, що може привести до порушення управління.

Загроза безпеці виступає в якості можливості вирішення протиріччя у взаємодії об'єкта безпеки та/абр його компонентів з іншими об'єктами шляхом нанесення йому (їм) шкоди.

Загроза інформаційній безпеці – сукупність умов і факторів, що визначають потенційну або реально існуючу можливість порушення конфіденційності, цілісності, доступності та спостережності інформації та/або зменшення надійності [безвідмовності та аутентичності] реалізації функцій системи на об'єкті безпеки.

ЕВОЛЮЦІЯ ЗАГРОЗ

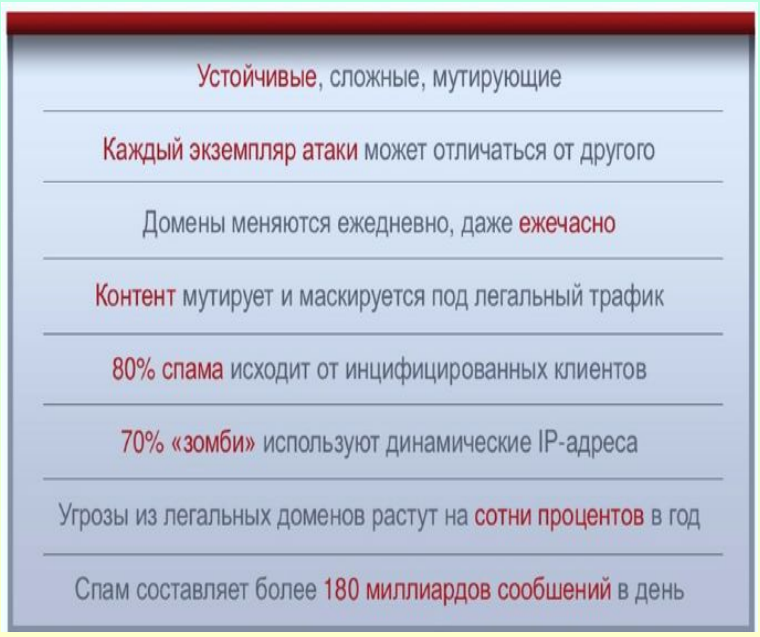
ДЖЕРЕЛА ЗАГРОЗ

Люди → **Сторонні особи, Користувачі, Персонал**
Технічні пристрої → **Реєстрації, Передачі, Зберігання, Переробки, Видачі**
Моделі, алгоритми, програми: допоміжні; прикладні ; загал. призначення
Технологічні схеми обробки: ручні, інтеракт., внутрішньо-машинні, мережні
Зовнішнє середовище: стан атмосфери, побічні шуми, побічні сигнали

ПРИРОДА ПОХОДЖЕННЯ ЗАГРОЗ :

Випадкова → **Відмови: (збої, помилки, стихійні лиха, побічні впливи)**
Навмисна → **Злочинні дії людей**

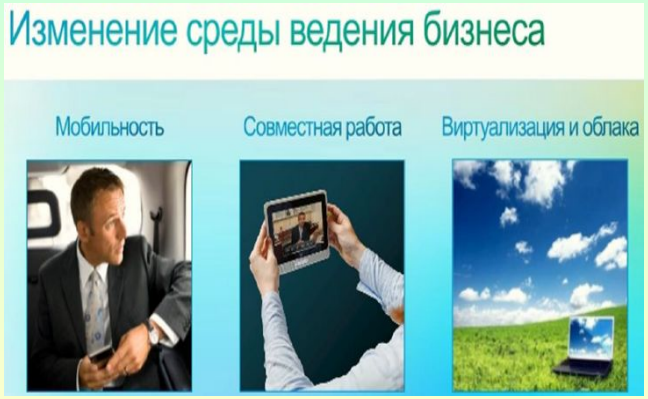
ЗАГРОЗИ СЬОГОДНІ



ПЕРЕДУМОВИ ПОЯВИ ЗАГРОЗ

Об'єктивні
→ Кількісна недостатність елементів системи
→ Якісна недостатність елементів системи
Суб'єктивні
→ Розвідувальні органи іноземних держав
→ Промислове шпигунство
→ Карні елементи
→ Несумлінні співробітники

ПРИЧИНИ ПОЯВИ НОВИХ ЗАГРОЗ



Основні методи та способи реалізації загроз

Способи реалізації загроз:

шкідливе ПЗ (Malware);
інтернет-шахрайство;
НСД до IP та ІТС;
бот-мережі (botnet);
DDoS-атаки;
крадіжка особистості ...

Основні методи реалізації загроз

Уровень доступа информации	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступности
Носителей информации.	Определение типа и параметров носителей информации.	Хищение (копирование) носителей информации; перехват ПЭМИН.	Уничтожение машинных носителей информации.	Выведение из строя машинных носителей информации.
Средств взаимодействия с носителем.	Получение информации о программно-аппаратной среде; получение детальной информации о функциях, выполняемых системой; получение данных о применяемых системах защиты.	Несанкционированный доступ к ресурсам системы; совершение пользователем несанкционированных действий; несанкционированное копирование программного обеспечения; перехват данных, передаваемых по каналам связи.	Внесение пользователем несанкционированных изменений в программы и данные; установка и использование нештатного программного обеспечения; заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент системы; обход механизмов защиты.
Представления информации.	Определение способа представления информации.	Визуальное наблюдение; раскрытие представления информации (дешифрование).	Внесение искажения в представление данных; уничтожение данных.	Искажение соответствия синтаксических и семантических конструкций языка.
Содержания информации.	Определение содержания данных на качественном уровне.	Раскрытие содержания информации.	Внедрение дезинформации.	Запрет на использование информации.

Шкідливе ПЗ (Malware)

- віруси;
- мережеві хробаки (networm);
- троянські програми (trojan);
- руткіти (rootkit);
- клавіатурні шпигуни (keylogger);
- рекламні системи (adware)

Інтернет-шахрайство

-фішинг (phishing). Атака полягає у спонуканні користувача ввести свої автентифікаційні дані (логін, пароль тощо) та іншу інформацію шляхом запевнення останніх щодо достовірності та справжності хибних (спеціально створених для цього) мережевих ресурсів, таких як пошта, веб-сайти, призначені для Інтернет-банкінгу, сторінки авторизації у соціальних мережах тощо;

- ***вішинг (vishing).*** Вид шахрайства, що полягає в отриманні у користувача під час телефонної розмови, шляхом використання різних методів перекона ння, необхідної зловмиснику інформації.

Несанкціонований доступ до IP та ІТС

1) цілеспрямована хакерська атака - дії, спрямовані на пору-шення штатного режиму функціонування системи, порушення досту-пності її сервісів (компонентів), отримання несанкціонованого досту-пу до конфіденційної інформації, порушення її цілісності тощо.

2) дефейс - атака, що полягає у зміні змісту головної сторінки веб-сайту, в результаті чого при його відвідуванні замість звичного контенту відображається щось інше (написи «Hacked By», нецензурні або провокаційні фрази/малюнки).

Типові шляхи реалізації НСД до IP:

·перехват электронных излучений;
·принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;
·применение подслушивающих устройств (закладок);
·дистанционное фотографирование;
·перехват акустических излучений и восстановление текста принтера;
·хищение носителей информации и документальных отходов;
·чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

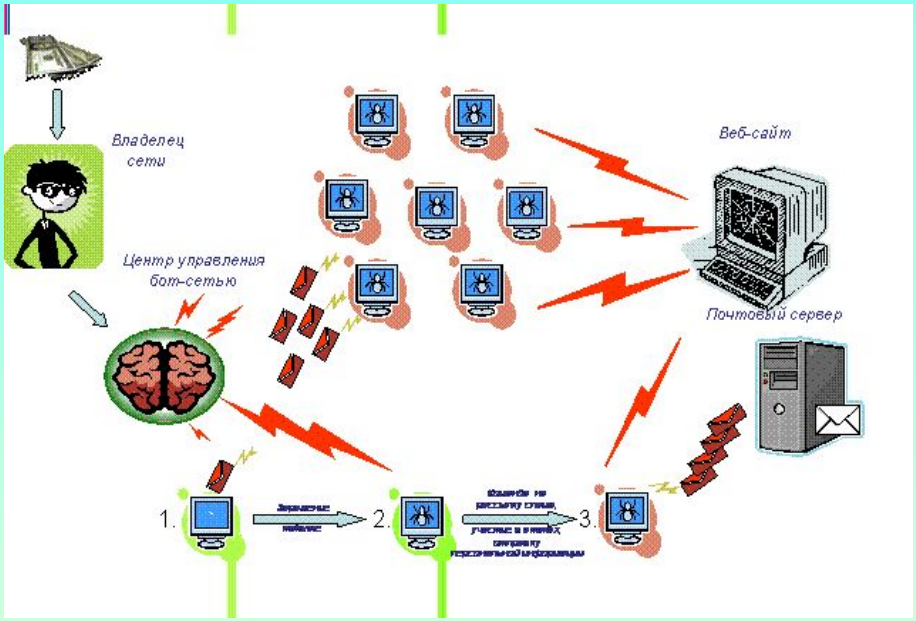
Типові шляхи реалізації НСД до IP:

·копирование носителей информации с преодолением мер защиты;
·маскировка под зарегистрированного пользователя;
·мистификация (маскировка под запросы системы);
·использование программных ловушек;
·использование недостатков языков программирования и операционных систем;
·включение в библиотеки программ специальных блоков типа "Троянский конь";
·незаконное подключение к аппаратуре и линиям связи;
·злоумышленный вывод из строя механизмов защиты;
·внедрение и использование компьютерных вирусов.

Способи реалізації загроз

Бот мережі (botnet)

Сукупність комп'ютерів, уражених шкідливим програмним забезпеченням, ресурси яких (як інформаційні, так і виробничі) через спеціальні командно-контрольні сервери (C&C) несанкціоновано використовуються зловмисниками (ZeuS, SpyEye, Carberp, Rustock, Kelihos, Pandora, BlackEnergy …)



«Крадіжка особистості»

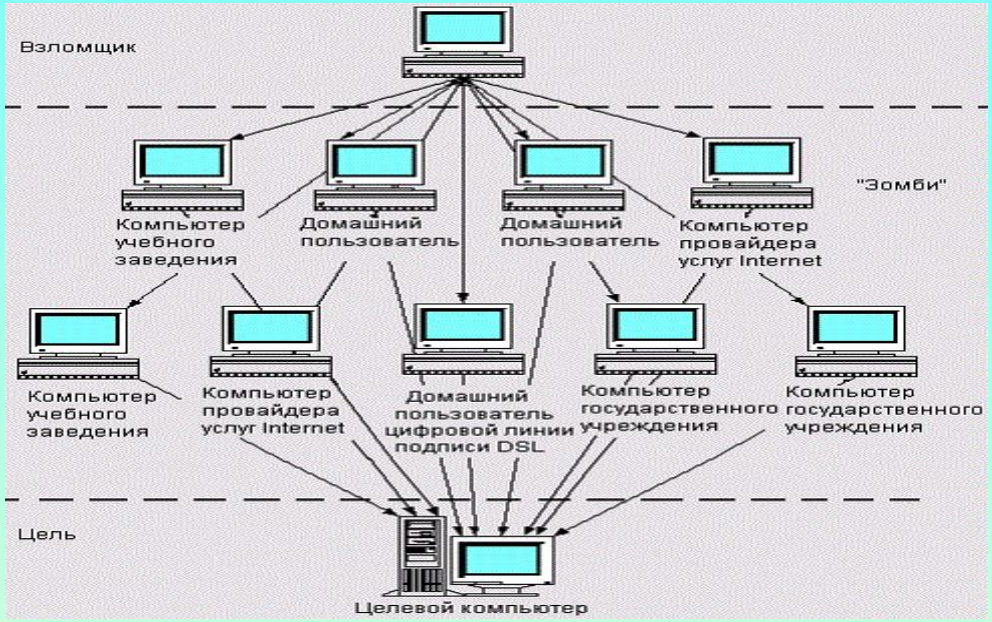
Несанкціоноване заволодіння персональ-ними даними особи, що дозволяє зловмис-нику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами тощо) від її імені (як один із механізмів підтвердження автентичності особи може використовуватись електронний цифровий підпис).

Розсилання спаму

У результаті реалізації зазначеної атаки «рядові» користу-вачі отримують у значній кількості на свої електронні пош-тові скриньки повідомлення, які ними не очікувались та які містять інформацію рекламного та/або шахрайського характеру.

DDoS-атака

Розподілена мережева атака, яка за допо могою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів.



Атака на відмову в обслуговуванні

Обьект защиты: трафик, предназначенный для переполнения атакуемой сети, необходимо "отсекать" у провайдера услуг Интернет. Когда атака этого типа проводится одновременно через множество устройств, говорится о **распределенной атаке** DoS (Distributed Denial of Service — DDoS).

Основные способы защиты:

1. **П**равильно сконфигурировать функции анти-спуфинга на маршрутизаторах и межсетевых экранах. Если хакер будет не в состоянии замаскировать свою истинную личность, он вряд ли решится на проведение атаки.
2. **В**ключить и правильно сконфигурировать функции анти-DoS на маршрути-заторах и межсетевых экранах.
3. **О**граничить объем проходящего по Сети некритического трафи-ка. Об этом нужно договариваться с Интернет-провайдером.

Модель загроз та модель порушника

Модель нарушителя

Носители	Квалификация	Средства
Хактивист	Студент	Общедоступные
Организованная преступность	Специалист	Специализированные
Инсайдер	Профессионал или сообщество	Таргетированные или не опубликованные
Шпионаж		
Военный хакинг		

Модель угроз

Технические средства:

DE	Data Encryption
VMS	Vulnerability Management
NGFW	Next Generation Firewall
SIEM	Security Event and Incident Management
DBS	Data Base Security
IDM	Identity Management
WSG	Web Security Gateway
DLP	Data Loss Prevention

Организационные меры:

- Формализация процессов ИБ
- Инвентаризация и классификация ресурсов
- Анализ рисков ИБ
- Повышение осведомленности пользователей
- Дисциплинарный процесс

Еволюція тактики та таксономії реалізації загроз. Приклад.

У каждого своя роль

- Менеджер по продажам
- Кассир
- Маркетолог
- Логист
- Водитель
- HR
- Генеральный директор
- Айтишник
- Охранник
- Инженер
- Разработчик
- Дроп (разводной / неразводной)
- Дроповод
- Обнальщик
- Заливщик / Даунлоадер
- Селлер
- Abuse-хостер
- Гарант
- Кодер

ПЕРСОНАЛ

ПРИКЛАД реалізації загроз

Популярный пример жизненного цикла киберпреступности

1. Разработка и тестирование вредоносного кода
2. Вредоносный код объявляется к продаже
3. Вредоносный код размещается на различных сайтах
   - Сайты могут быть как специально подготовленные, так и общепопулярные, но взломанные
4. Вредоносный код загружается на компьютеры пользователей при посещении зараженных сайтов
   - В случае специально подготовленных сайтов используются партнерские схемы pay-per-install
5. Вредоносный код собирает информацию для продажи (учетные записи, персональные данные, ключи электронной подписи и т.д.)
6. Собранная информация используется или продается

Ключевые партнеры

- Оптимизация и экономия в сфере производства
- Снижение риска и неопределенности
- Поставки ресурсов и совместная деятельность

- Типы партнеров
  - Abuse-хостеры
  - Гаранты
  - Владельцы ботнетов
  - Владельцы анонимных прокси
  - Владельцы Fast-Flux-хостинга
  - Продавцы трафика
  - И т.д.

Массовое заражение → **Полиморфизм** → **Фокус на конкретную жертву** → **Передовые и тайные средства (APT)**

Злоумышленников не интересует известность и слава – им важна финансовая выгода от реализации угрозы

Современные угрозы постоянно меняются, чтобы средства защиты их не отследили – изменение поведения, адресов серверов управления

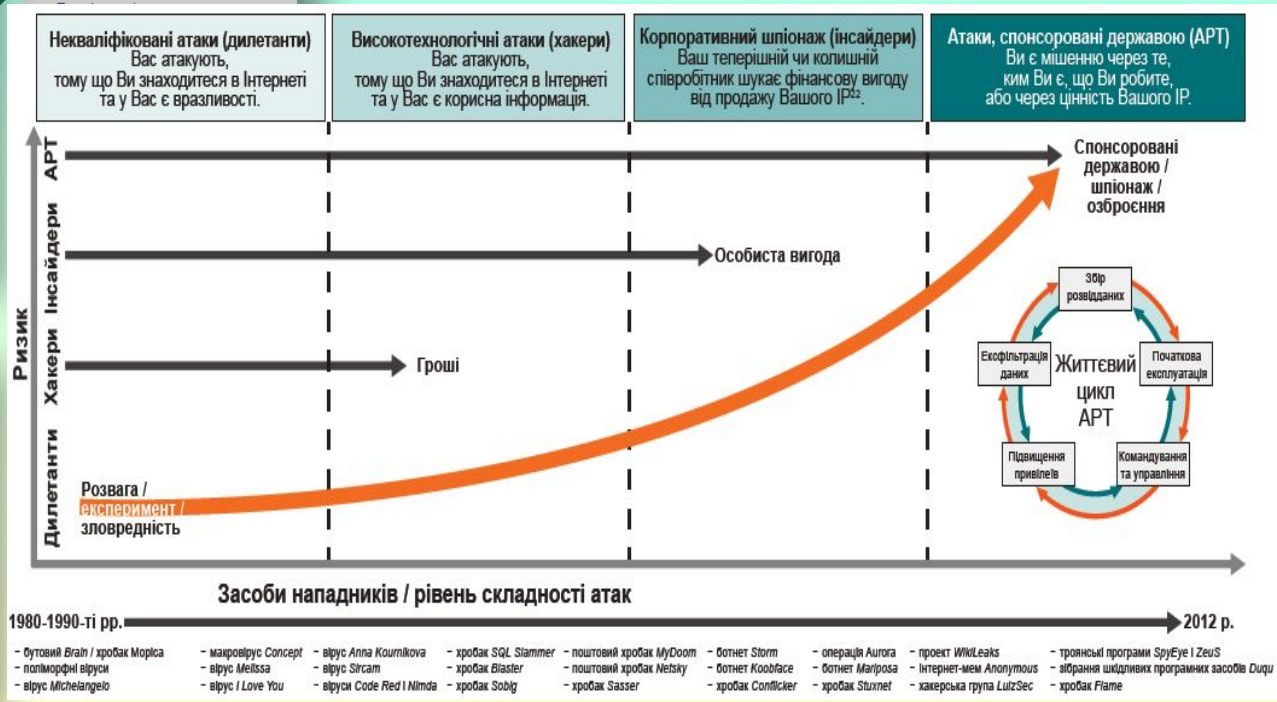
Угрозы могут быть разработаны специально под вас – они учитывают вашу инфраструктуры и встраиваются в нее, что делает невозможным применение стандартных методов анализа

Угрозы становятся модульными, самовосстанавливающимися и устойчивыми к отказам и обнаружению

Ключевые виды деятельности

- Производство
- Разрешение проблем

Еволюція тактики та таксономії реалізації загроз

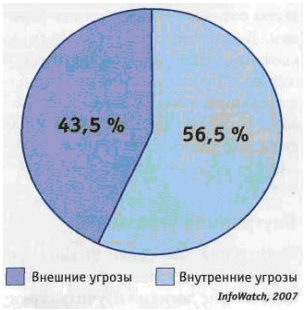


Систематизація (класифікація) та зміна ландшафту загроз безпеці ІТС

Систематизація – приведення в систему, тобто в дещо ціле, що являє собою єдність закономірно розташованих частин, які знаходяться у взаємозв'язку та налаштування їх у визначеному порядку.

ВИДИ КЛАСИФІКАЦІЇ ЗАГРОЗ БЕЗПЕЦІ

- Класифікація загроз за місцем знаходження їхнього джерела
  - Зовнішні загрози
  - Внутрішні загрози
- Класифікація загроз за сформованістю
  - Потенційна загроза
  - Реальна загроза
- Класифікація загроз за характером їхнього суб'єктивного сприйняття
  - Завищена та занижена загрози
  - Умовна загроза
  - Адекватна загроза
- Класифікація загроз за характером їхнього виникнення
  - Соціального характеру
    - Соціальний конфлікт
  - Техногенного характеру
    - Надзвичайна ситуація
    - Аварія
    - Катастрофа
  - Природного характеру
    - Стихійні лиха
- Класифікація загроз за за сферами людської діяльності
  - Основні сфери людської діяльності: політична, оборонна, економічна, соціальна, міжнародна, екологічна, інформаційна

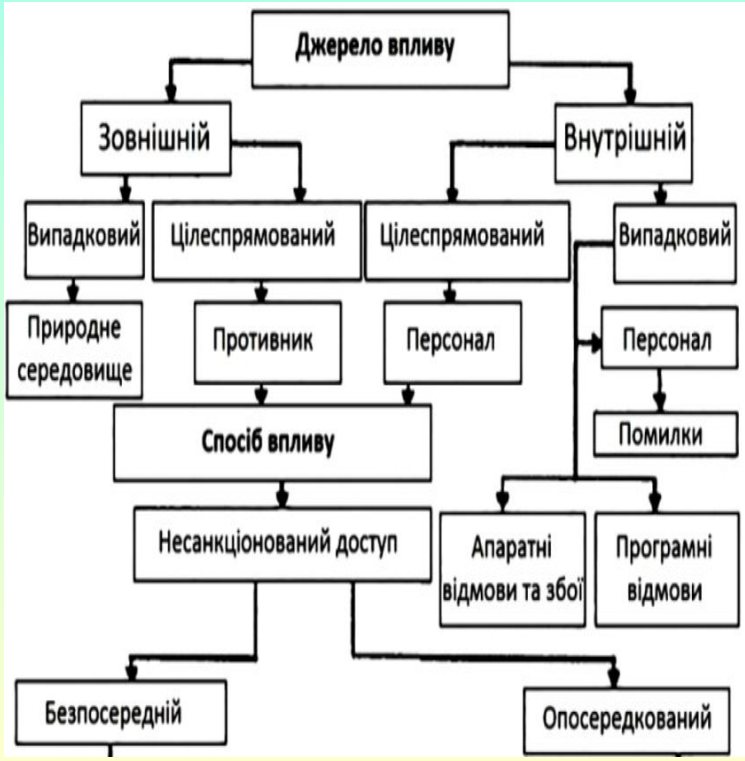


Приклад співвідношення внутрішніх і зовнішніх загроз

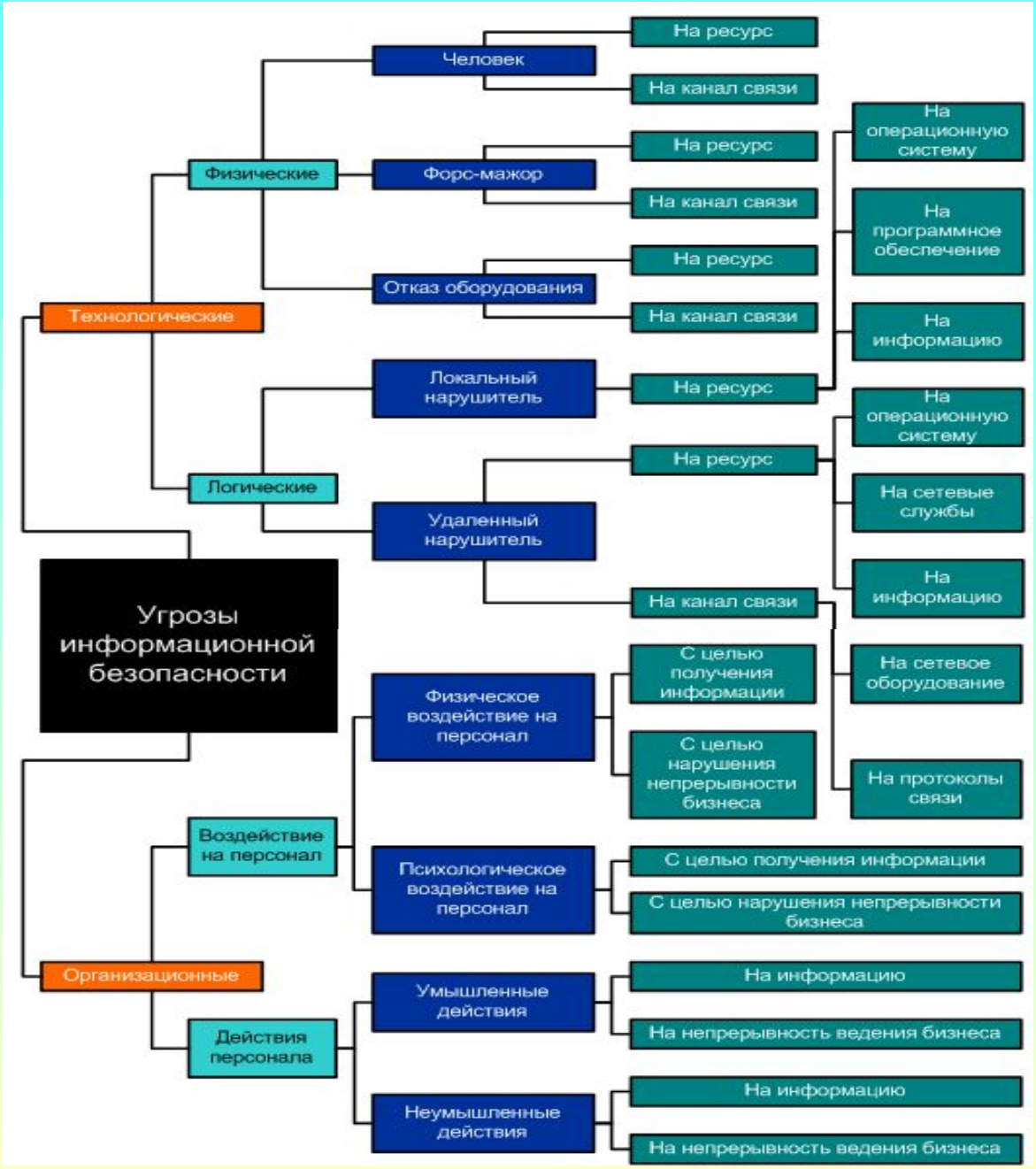
Приватним випадком систематизації є класифікація

КЛАСИФІКАЦІЯ **–**
послідовне ділення понять, що проводиться по характеристикам і параметрам, існуючим з точки зору досліджуваної задачі

Виділяють:
- **таксономічну (род-вид) класифікацію;**
- **мереологічну (частина-ціле);**
- **фасетну (аналітико-синтетичну).**

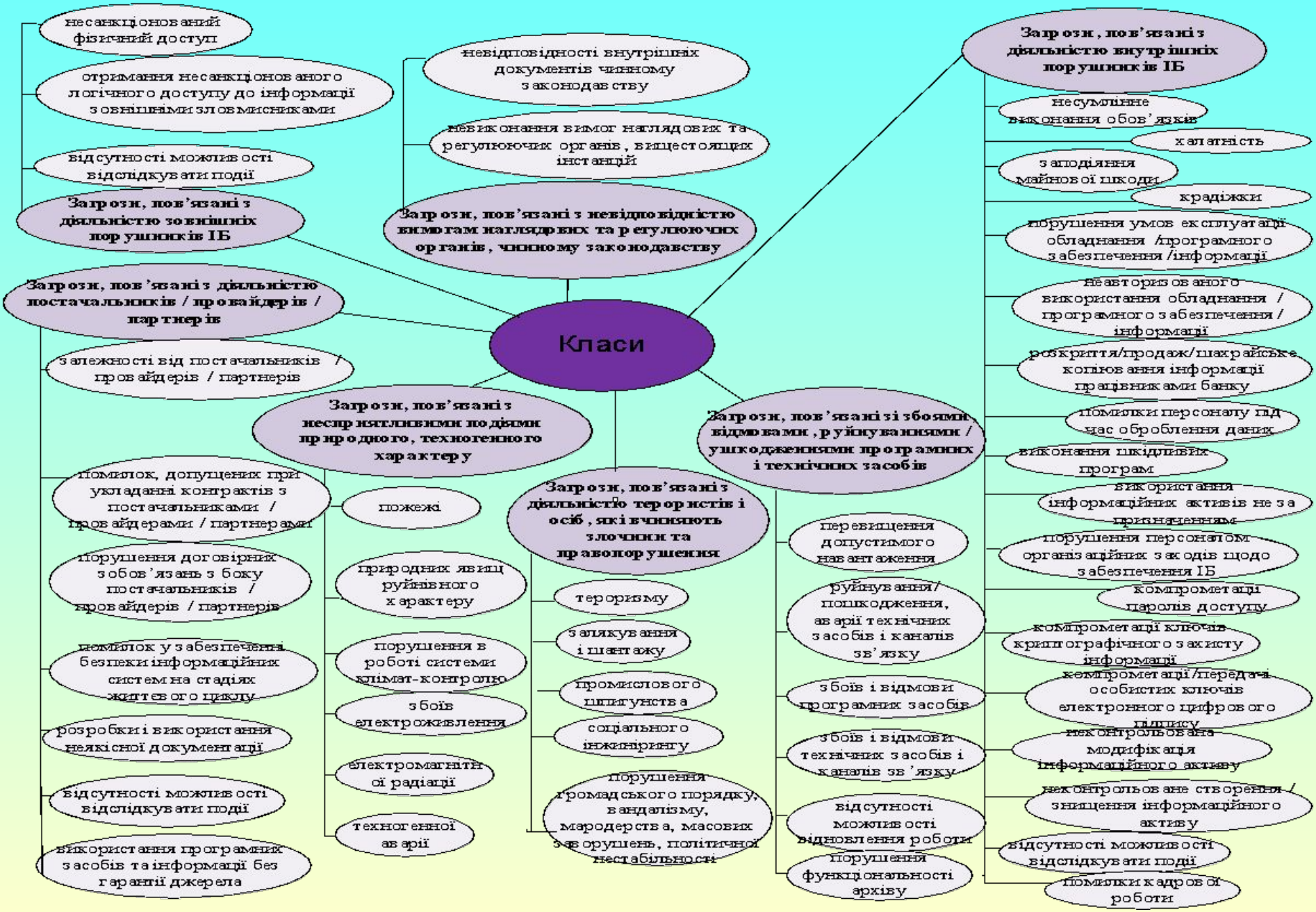


Класифікація загроз за видами ознак



За характером порушення	•порушення конфіденційних даних •порушення працездатності КС •незаконне втручання в функціонування КС
За тяжкістю порушення	•незначні помилки •дрібне хуліганство •серйозний злочин
По передбаченню наслідків порушників	•умисне порушення •не умисне
За мотивацією	•зловмисне •незловмисне
За місцем виникнення	•зовнішні загрози •внутрішні(загрози за сторони інсайдерів)
За закінченістю	•реалізовані •не реалізовані
За обєктом впливу	•загрози, націлені на всю інформаційну систему •загрози, націлені на окремі компоненти інформаційної системи
За причиною виникнення	•загрози, що виникли в результаті недостатніх засобів технічного захисту •загрози, що виникли через брак організаційних мір
За каналом проникнення	•через слабкість програмного забезпечення •через прогалини в системі авторизації, недоліки системи зберігання документів
За видом релізації загрози	•шкідливі програми, спам, програмні закладки, хакерські атаки •уразливі процедури авторизації та інші регламенти інформаційної безпеки
За походженням	•стихійні лиха •антропогенні •техногенні •природні
За розміром збитку	•незначні •значні •критичні

Класифікація загроз за видами діяльності



Каталогізація загроз та їх головні аспекти

Каталогізація загроз в продуктах і системах IT

- **Загрози даним на носіях**
- **Загрози даним в телекомунікаційних лініях**
- **Загрози прикладним програмам (додаткам)**
- **Загрози прикладним процесам і даним**
- **Загрози даним, що віддзеркалюються**
- **Загрози даним, що вводяться**
- **Загрози даним, що виводяться на друк**
- **Загрози данным користувачів**
- **Загрози системним службам і даним**
- **Загрози інформаційному обладнанню**

Аспекти загрози

- джерело впливу (люди, інші фактори)
- передбачуваний метод (спосіб, особливості) впливу
- уразливості, які м.б. використані для реалізації впливу
- об'єкти (активи), що можуть бути піддані впливу

	...ління
	...вління
	...довищу) передачі
За уразливостями (системи та її елементів), що використовуються	загрози, що реалізуються за рахунок уразливостей складових КС
	загрози, що реалізуються за рахунок використання уразливостей системи захисту КС (за наявності такої системи)
	загрози, що реалізуються із застосування недоліків в алгоритмах управління й обробки інформації
За способом реалізації	загрози, що передбачають актине втручання у процес функціонування КС та її складових (активні КС)
	загрози, що безпосередньо не впливають на роботу КС (пасивні КЗ)
	загрози з комплексним характером впливу
За доцільністю реалізації	можливі, але малоймовірні
	з високою ймовірністю реалізації
За часом виникнення	загрози, які закладено при створенні КС
	загрози, що виникли під час функціонування КС
За повторюваністю появи	повторювані (періодичні, аперіодичні)
	неповторювані

За видом КС	технічні
	біологічні
	соціальні
	комбіновані
За середовищем поширення	інформаційні
	комунікаційні
	комп'ютерно-мережні
	соціотехнічні
За умисністю	навмисні
	ненавмисні
За прихованістю прояву	приховані
	неприховані
За розташуванням джерела КЗ	внутрішні
	зовнішні
За походженням	природного походження
	штучного походження
За масштабами наслідків від реалізації загрози	локальні
	частковосистемні
	загальносистемні
За ієрархією управління	вищого (стратегічного) рівня
	середнього (оперативного) рівня
	нижчого (тактичного) рівня
За умовністю реалізації	умовні
	безумовні

Типи загроз безпеки інформації в ІТС

Тип загрози		Причини або спонукальні мотиви
Навмисні загрози	Ненавмисні загрози	
Розкрадання носіїв інформації	-	Прагнення використовувати конфіденційну інформацію у своїх цілях
Застосування програмних пасток	-	
-	Несправність апаратури, що може ініціювати несанкціоноване зчитування ІР	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Використання програм "троянський кінь"	-	Завдання збитків шляхом несанкціонованого доступу в систему
Помилки в програмах обробки інформації	-	Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп'ютерного вірусу	-	Руйнування інформаційної системи з метою завдання збитків
-	Помилки в програмах обробки інформації	Застосування несертифікованого програмного продукту
-	Впровадження комп'ютерного вірусу	Не дотримання обслуговуючим персоналом вимог безпеки, порушення ним технологічної послідовності роботи із системою
Помилкова комутація в мережі ЕОМ	-	З метою створення каналу для витоку конфіденційної інформації
-	Помилкова комутація в мережі ЕОМ	Низька кваліфікація обслуговуючого персоналу
-	Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування інформаційної системи або її створення
-	Перехресні наведення за рахунок ЕМВ	
Примусове електромагнітне опромінення	-	Вивід з ладу інформаційної системи з метою завдання збитків
Використання акустичних випромінювань	-	Одержання конфіденційної інформації
Копіювання за допомогою візуального й слухового контролю	-	
Маскування під користувача, підбор пароля	-	Несанкціоноване втручання в роботу системи в злочинних цілях
-	Помилка в роботі оператора	Низька кваліфікація оператора, застосування несертифікованого ПЗ
-	Помилки користувача	Використання недостатнього захисту
Помилки програміста: опис і перекручування програмного захисту, розкриття кодів та паролів	-	З метою добування особистої вигоди або завдання збитків
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація	-	-
-	Помилки персоналу: перекручування схем захисту, помилкова комутація	Недостатня кваліфікація, порушення технології

Перелік можливих загроз ІР, що циркулює та обробляється в ІТС

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденцій ність	Цілісність	Доступність	Спостереж-
Загрози природного походження							
1	Катастрофа	Пожежа, повінь, землетрус, ураган, вибух	Середовище		+	+	
2	Умови	Вологість, запиленість, зміни температури	Середовище		+	+	
Випадкові загрози техногенного походження							
3	Вібрація	Вібрація	Апаратура		+	+	
4	Перешкоди	Небажаний вплив процесів один на одного	Апаратура		+	+	
5	ЕМВ	Зовнішні електромагнітні випромінювання (електромагнітна сумісність)	Апаратура		+	+	
6	Аварія	Аварія систем життєзабезпечення.	Середовище		+	+	
7	Відмова-Л	Відмови (повний вихід з ладу, систематичне неправильне виконання своїх функцій) людей	Люди			+	+
8	Відмова-А	Відмови основної апаратури, систем передачі даних, носіїв інформації	Апаратура		+	+	+
9	Відмова-П	Відмови програм	Програми		+	+	+
10	Відмова-З	Відмови систем живлення, систем забезпечення нормальних умов роботи апаратури й персоналу (електроживлення, охолодження й вентиляції, ліній зв'язку тощо).	Середовище, апаратура		+	+	
11	Збій-А	Збої основної апаратури систем передачі даних	Апаратура	+	+	+	+
12	Збій-З	Збої систем харчування, систем забезпечення нормальних умов роботи апаратури й персоналу	Середовище, апаратура		+	+	
13	Помилка-Л	Випадкові помилки користувачів, що обслуговує персоналу, помилкова конфігурація й адміністрування системи	Люди	+	+	+	+
14	Помилка-П	Помилки програм	Програми	+	+	+	+
15	Недбалість	Недбале зберігання й облік документів, носіїв інформації	Люди	+	+	+	+
16	Поломка-А	Поломка апаратури.	Люди	+	+	+	
17	Поломка-Н	Ушкодження носіїв інформації	Люди, апаратура		+	+	

Перелік можливих загроз ІР, що циркулює та обробляється в ІТС

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
18	Вірус	Поразка програмного забезпечення комп'ютерними вірусами.	Люди, програми	+	+	+	+
19	Підключення	Підключення до каналів зв'язку через штатні або спеціально розроблені апаратні засоби (у тому числі підключення через установлені модемні, факс- модемні плати)	Люди, апаратура, програми	+		+	
Навмисні загрози техногенного походження дистанційної дії							
20	ПЕМВ	Одержання інформації з каналу побічного електромагнітного випромінювання основних технічних засобів (пристроїв наочного відображення, системних блоків, периферійної апаратури, апаратури зв'язку, ліній зв'язку, кабелів)	Апаратура	+			
21	Е-наведення	Одержання інформації з каналу побічних наведень у системах каналізації, у мережах теплопостачання, у системах вентиляції, у шинах заземлення, у мережах харчування,у ланцюгах телефонізації	Апаратура	+			
22	Віброакустика	Одержання інформації з віброакустичного каналу з використанням лазерних пристроїв зняття інформації	Апаратура	+			
23	Спецвпливи	Одержання інформації з каналів спеціального впливу (електромагнітне й високочастотне опромінення об'єкта захисту)	Апаратура	+			
24	Е-імпульс	Використання електромагнітних імпульсів з метою знищення інформації, засобів її обробки й зберігання	Апаратура		+	+	
25	Підслуховування-Т	Прослуховування телефонних мереж	Апаратура, люди	+			
26	Оптика	Використання оптичних засобів, дистанційне фотографування	Апаратура	+			
27	НСД-ЛВЗ	Несанкціонований дистанційний доступ до ЛВЗ	Люди, апаратура, програми	+	+	+	+
28	Переадресація	ере адресація (зміна маршруту) передачі даних.	Люди, програми	+		+	+
29	Нав'язування	Нав'язування порочної інформації під ім'ям авторизованого користувача	Люди, програми		+		+

Перелік можливих загроз ІР, що циркулює та обробляється в ІТС

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
Навмисні погрози техногенного походження контактної дії							
30	Прослуховування	Прослуховування мережі за допомогою програмних або програмно- апаратних аналізаторів.	Апаратура, програми	+			+
31	Читання-З	Читання "сміття" (залишкової інформації із запам'ятовувальних пристроїв)	Люди, апаратура, програми	+			
32	Читання-Е	Оглядання даних, які виводяться на екран.	Люди, апаратура	+			
33	Читання-Д	Оглядання даних, які роздруковуються, читання залишених без огляду видрукуваних на принтері документів	Люди, апаратура	+			
34	Ушкодження	Фізичне знищення системи (у результаті вибуху, підпалу й т.п.), ушкодження всіх або окремих найбільш важливих компонентів АС (прибудував, носіїв важливої системної інформації, осіб із числа персоналу й т.п.), систем електроживлення тощо	Люди		+	+	
35	Відключення-О	Відключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження й вентиляції, ліній зв'язку тощо)	Люди, апаратура, програми		+	+	
36	Закладка	Використання й дистанційні пристрої, що підслуховують.	Люди, апаратура	+			
37	Випитування	Провокація до розмов осіб, що мають відношення до АС.	Люди	+			+
38	Копіювання	Копіювання вихідних документів, магнітних і інших носіїв інформації (у тому числі при проведенні ремонтних і регламентних робіт із ГМД)	Апаратура, програми, люди	+			
39	Розкрадання	Розкрадання магнітних носіїв і документів (оригінали й копії інформаційних матеріалів, ГМД, стрімерних стрічок), виробничих відходів (відбитків, записів, носіїв інформації т.п.), одержання неврахованих копій	Люди	+			
40	Імітація	Незаконне одержання паролів і інших реквізитів розмежування доступу (агентурним шляхом, у результаті недбалості користувачів, підбором, імітацією інтерфейсу системи тощо) з наступним маскуванням під зареєстрованого користувача ("маскарад")	Люди, програми	+	+		+

Перелік можливих загроз ІР, що циркулює та обробляється в ІТС

№ з/п	Позначення загроз	Тип і визначення загроз	Джерело загроз	Наслідки			
				Конфіденційність	Цілісність	Доступність	Спостережність
41	НСД-РС	Несанкціоноване використання робочі станції й терміналів ЛВЗ	Люди програма	+	+	+	+
42	НСД-П	Несанкціоноване використання технічних засобів (модем, апаратний блок кодування, периферійні пристрої)	Люди програми	+		+	+
43	Злом	Обхід механізмів захисту з метою забезпечити надалі псевдосанкціонований доступ порушника	Люди програми	+	+		
44	Перехоплення	Перехоплення паролів програмою-імітатором, перехоплення повідомлень.	Люди, програми	+	+	+	+
45	Закладка-П	Включення в програми програмних закладок типу "троянський кінь", "бомба" тощо.	Люди, програми	+	+	+	+
46	Підміна	Несанкціоновані зміни, підміна елементів програм, елементів баз даних, апаратури, магнітних носіїв.	Люди, програми	+	+	+	+
47	Дезорганізація	Дії щодо дезорганізації функціонування системи (зміна режимів роботи пристроїв і програм, страйк, саботаж персоналу, постановка потужних активних перешкод на частотах роботи пристроїв системи й т.п.)	Люди, програми		+	+	
48	Вербування	Вербування персоналу або окремих користувачів, які мають певні повноваження	Люди	+	+		
49	Вади	Використання вад немов програмування, операційних систем (у тому числі параметрів системи захисту, установлених "за замовчуванням").	Люди, програми	+	+	+	+

Конфіденційність інформації

свойство информации,субъективно устанавливаемое ее собственником, когда ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц, при условии того, что собственник принимает меры по организации доступа к информации только уполномоченных лиц

Загроза безпеці інформації -
сукупність умов і факторів (явищ, дій чи процесів), що створюють потенційну або реально існуючу небезпеку, в результаті якої можливі витік інформації, неправомірне модифікування (спотворення, підміна), знищення інформації або неправомірне блокування доступу до неї.

Загрози конфіденційності інформації

Загрози цілісності інформації

Загрози доступності інформації

Витік інформації -
неконтрольоване розповсюдження інформації в результаті її розголошення, несанкціонованого доступу до неї або отримання інформації, що захищається іноземними розвідками та іншими зацікавленими суб'єктами (зацікавленими суб'єктами можуть бути: держава, юридична особа, група фізичних осіб, окрема фізична особа).

Неправомірний вплив на інформацію -
фактори (явище, дія або процес), результатом яких можуть бути неправомірне знищення, неправомірне модифікування (спотворення, підміна) інформації або неправомірне блокування доступу до інформації.

Цілісність інформації

неискаженность, достоверность, полнота, адекватность и т.д., т.е. такое свойство информации, при котором ее содержание и структура (данных) определены уполномоченными лицами и процессами

Доступність інформації

свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию собственником или уполномоченными лицами

Загрози витоку інформації та неправомірного впливу на неї

Витік інформації

Розголошення інформації (відомостей) -

таке протиправне оприлюднення цих відомостей, при якому вони стали надбанням сторонніх осіб (при цьому стороннім визнається будь-яка особа, яка за характером виконуваної роботи або службових обов'язків не має доступу до даних відомостей)

- Навмисне розголошення (прямий умисел).
- Ненавмисне розголошення (з необережності)

Несанкціонований доступ до інформації (НСД) -

доступ до інформації, здійснюваний з порушенням встановлених прав і (або) правил доступу до інформації із застосуванням штатних засобів, що надаються СВТ або АС, або засобів, аналогічних їм за своїми функціональним призначенням та технічними характеристиками

- Фізичний доступ.
- Програмно-апаратний доступ.
- Програмний доступ

Перехоплення інформації (витік інформації технічними каналами) -

неправомірне отримання інформації з використанням технічного засобу, який здійснює виявлення, приймання та обробку інформативних сигналів

- Перехоплення інформації, яка обробляється технічними засобами.
- Перехоплення розмов, що ведуться у виділених (які захищаються) приміщенн
- Перехоплення інформації, переданої по каналах зв'язку

Розкрадання носія інформації

Неправомірний вплив на інформацію

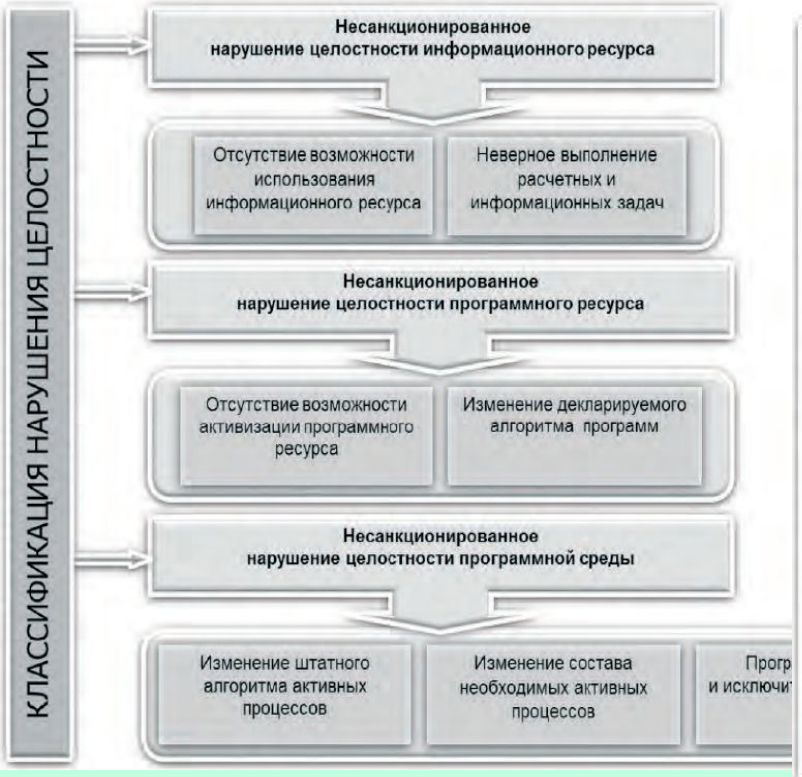
Умисний вплив:

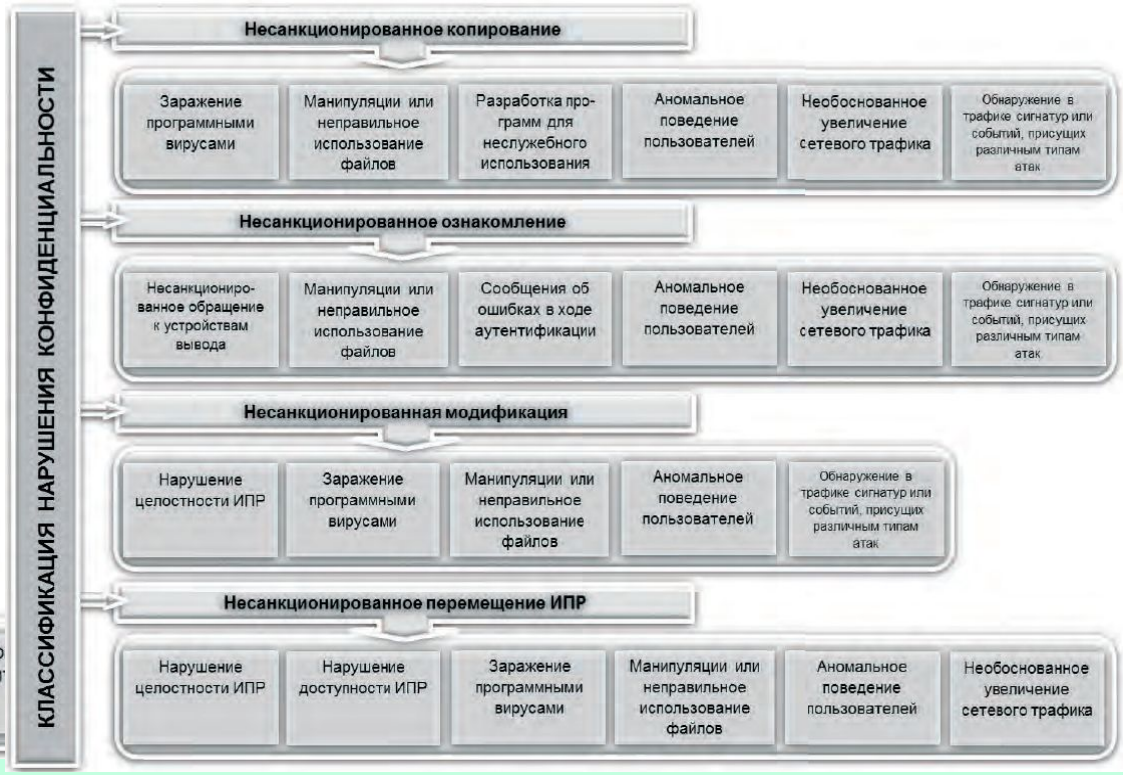
- Диверсія щодо ОІ, в результаті якої відбулося руйнування, знищення інформації, носія інформації або ТСОІ;
- Використання спеціальних програмних впливів на інформацію (шкідливих програм, програмних закладок та комп'ютерних вірусів), що викликають зміну (спотворення, підміну), знищення інформації або блокування доступу до неї;
- Використання спеціальних програмних впливів на програмне забезпечення ТСОІ, що викликають блокування доступу до інформації, збої в роботі ТСОІ або функціонуванні носія інформації;
- Впровадження в ТСОІ закладних пристроїв, що викликають зміну (спотворення, підміну), руйнування, знищення інформації або блокування доступу до неї;
- Впровадження в ТСОІ закладних пристроїв, що викликають блокування доступу до інформації, збої в роботі ТСОІ або функціонуванні носія інформації;
- Навмисне силове електромагнітний вплив із застосуванням технічних засобів, що викликає руйнування, знищення інформації або збої в роботі ТСОІ або функціонуванні носія інформації;
- Радіоелектронне придушення систем телекомунікації та зв'язку із застосуванням технічних засобів, що викликає модифікування (спотворення, підміну) або знищення інформації, переданої по каналах зв'язку.

Ненавмисний вплив:

- Явища техногенного характеру (ненавмисне електромагнітне опромінення ТСОІ, радіаційне опромінення ТСОІ, збої, відмови і аварії систем забезпечення ОІ);
- Природні явища, стихійні лиха (пожежі, повені, землетруси, грозові розряди);
- Дефекти, збої, відмови, аварії ТСОІ та програмного забезпечення;
- Помилки обслуговуючого персоналу ОІ (помилки при експлуатації ТСОІ і програмних засобів, помилки при експлуатації засобів і систем захисту інформації).

Ознаки порушення стану «ЦКД» інформації в ІТС





Формалізація процесів забезпечення ЦКДС IP в ІТС

CIA (Confidentiality, Integrity, and Availability — конфіденційність, цілісність та доступність) - три групи принципів, які є загальновизнаними при оцінюванні ризиків, повязаних з важливою інформацією, а також при формуванні політик безпеки.

я процесів формування
ібернетичної безпеки та
обґрунтування її коректності і
адекватності

КОНФІДЕНЦІЙНОСТІ

Організаційно-правові заходи та заходи фізичної безпеки

Ідентифікація та аутентифікація

Розмежування доступу

Криптографічні та стеганографічні методи

Методи захисту зовнішнього периметру

Протоколювання та аудит

МЕТОДИ, ЗАХОДИ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ

ДОСТУПНОСТІ

ЦІЛІСНОСТІ

Аутентифікація користувачів:
- мінімізація привілеїв;
- розподіл обов'язків.

Корегування транзакцій

Виявлення, протоколювання та аудит порушення цілісності

Криптографічні методи

Отримання інформації:
- дублювання «вузьких місць»;
- дублювання каналів зв'язку;
- підвищення пропускної спроможності мережевого обладнання.

Обробка інформації:
- дублювання серверів;
- використання кластерів;
- керування надійністю обладнання.

Передача інформації
- дублювання «вузьких місць»;
- дублювання каналів зв'язку;
- підвищення пропускної спроможності мережевого обладнання;
- динамічна маршрутизація.

Збереження інформації:
- резервне копіювання інформації;
- створення RAID-масивів;
- дзеркалювання серверів.

Загальний порядок виявлення актуальних загроз для ІТС

Якісна оцінка попереднього ступеня захищеності інформації в ІТС та переведення її в кількісну

↓

Формування переліку можливих загроз інформації в ІТС на основі базової моделі загроз

↓

Експертна якісна оцінка можливості реалізації кожної загрози й переведення її в кількісну

↓

Якісна оцінка ступеня небезпеки кожної загрози

↓

Прийняття рішення про віднесення кожної загрози до актуальної за встановленим правилом:

Актуальність загрози = можливість реалізації + ступінь небезпеки загрози

↓

Формування множини актуальних загроз

Можливість реалізації загрози:

- Рівень попереднього ступеня захищеності інформації в ІС (Y1)
- Частота (імовірність) реалізації загрози (Y2)

Рівень попереднього ступеня захищеності інформації в ІТС (Y1) передусім залежить від :

територіального розміщення;

наявності убудованих операцій із записами БД;

можливостей по розмежуванню доступу до інформації;

наявності з'єднань із іншими базами даних;

рівня узагальнення інформації;

обсягу інформації, надаваної стороннім користувачам без попередньої обробки.

ПРАВИЛО:

Якщо більше 70% характеристик відповідають рівню «високий» - ІТС має високий рівень захищеності (коеф. 0).

Якщо менш 70% характеристик відповідає рівню «високий» і не менш 70% відповідають рівню не нижче «середній» - ІТС має середній рівень захищеності (коефіцієнт 5).

Якщо не виконуються вказані вище умови - ІТС має низький рівень захищеності (коефіцієнт 10).

Під частотою (імовірністю) реалізації загрози (Y2) розуміється знайдений експертним шляхом показник, що характеризує наскільки ймовірним є реалізація конкретної загрози безпеки інформації для даної ІТС у певних умовах обстановки. Уводяться чотири вербальних градації цього показника:

малоймовірно - відсутні об'єктивні передумови для здійснення загрози (наприклад, загроза розкрадання носіїв інформації особами, що не мають легального доступу до приміщення, де останні зберігаються);

низька ймовірність - об'єктивні передумови для реалізації загрози існують, але вжиті заходи істотно утрудняють її реалізацію (наприклад, використані відповідні засоби захисту інформації);

середня ймовірність - об'єктивні передумови для реалізації загрози існують, але вжиті заходи забезпечення безпеки інформації недостатні;

висока ймовірність - об'єктивні передумови для реалізації загрози існують і заходи щодо забезпечення безпеки інформації не прийняті.

Загальний порядок виявлення актуальних загроз для ІТС

З урахуванням викладеного коефіцієнт реалізуємості загрози Y буде визначатися співвідношенням

$$Y = (Y1+Y2)/20.$$

За значенням коефіцієнта реалізуємості загрози Y формується вербальна інтерпретація реалізуємості загрози в такий спосіб:

- якщо $0<=Y<0,3$, то можливість реалізації загрози - низька;
- якщо $0,3<=Y<0,6$, то можливість реалізації загрози - середня;
- якщо $0,6<=Y<0,8$, то можливість реалізації загрози - висока;
- якщо $Y>=0,8$, то можливість реалізації загрози – дуже висока.

При оцінці ступеня небезпеки кожної загрози на основі опитування експертів (фахівців в області ЗІ) визначається вербальний показник небезпеки для розглянутої ІТС. Цей показник має три значення:

низька небезпека - якщо реалізація загрози може привести до незначних негативних наслідків;

середня небезпека - якщо реалізація загрози може привести до негативних наслідків;

висока небезпека - якщо реалізація загрози може привести до значних негативних наслідків.

Вибір із загального переліку загроз тих, які є актуальними для даної ІТС, здійснюється за такими правилами:

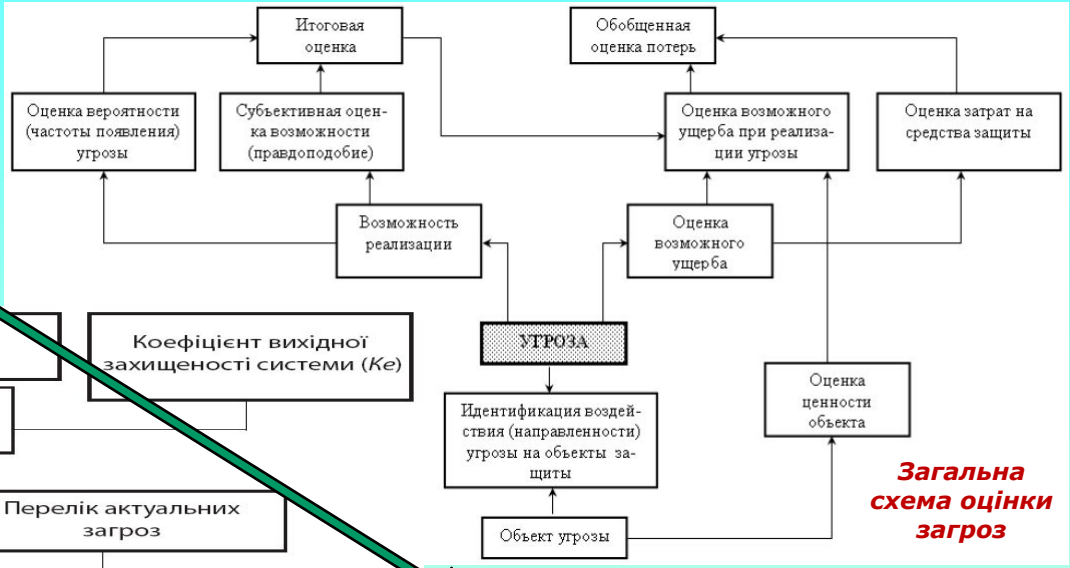
Можливість реалізації загрози	ПОКАЗНИК СТУПЕНЯ НЕБЕЗПЕКИ ЗАГРОЗИ		
	Низький	Середній	Високий
Мала	неактуальна	неактуальна	актуальна
Низька	неактуальна	актуальна	актуальна
Середня	актуальна	актуальна	актуальна
Висока	актуальна	актуальна	актуальна

Загрози витоку інформації технічними каналами й за рахунок НСД	Рівень попереднього ступеня захищеності (Y1)	Імовірність реалізації загрозы (Y2)				Коефіцієнт реалізації загрози Y=(Y1+Y2)/20	Показник ступеня небезпеки загрози			Висновок про актуальність загрози
		Мала (0)	Низька (2)	Середня (5)	Висока (10)	Можливість реалізації загрози	Низький	Середній	Високий	
Загрози витоку інформації по каналу ПЕМВН	5		2			0,35 середня	так			ні
Загрози витоку акустичної інформації	5	0				0.25 низька	так			ні
Загрози перехоплення паролей (ідентифікаторів)	5			5		0,5 середня			так	так

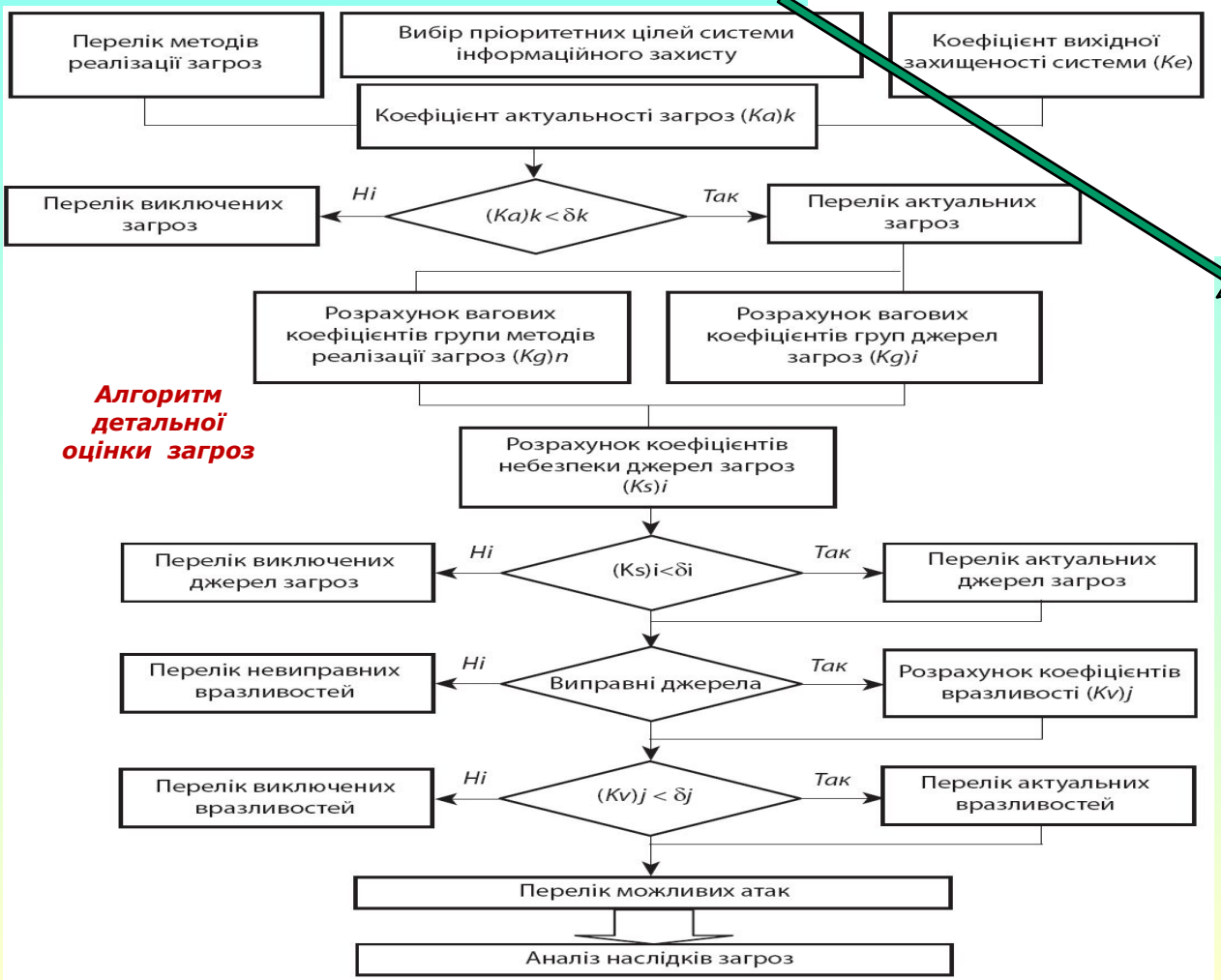
Загальна схема і алгоритм оцінювання загроз ІТС

Методы оценивания вероятности угроз

Апостериорные, на основе гистограмм распределения событий проявления соотв. угроз по результатам эксплуатации КС



Загальна схема оцінки загроз



Алгоритм детальної оцінки загроз

Априорные, на основе моделей и статистических характеристик физических процессов, реализующих соотв. угрозы (*z.b.* на основе Пуассоновского распределения вероятности моторных ошибок человека-оператора при вводе информации с клавиатуры с $\alpha = -2 \bullet 10^{-2} \ldots 4 \bullet 10^{-3}$)

Экспертные, на основе экспер-тных оценок специалис тов

Методы экспертного шкалирования

Методики экспертных оценок

1. Отбор экспертов (формальные и неформальные требования, метод «снежного кома», 10-12 экспертов)
2. Выбор параметров, по которым оцениваются объекты (стоимость, важность, веса параметров)
3. Выбор шкал оценивания (методов экспертного шкалирования)
4. Процедуры опроса экспертов (метод «Дельфи»)
5. Агрегирование оценок, анализ их устойчивости и согласованности

Примеры обработки угроз

Актуальные угрозы	Обоснование актуальности	Меры по устранению
Угрозы физического доступа к оборудованию АСУ ТП	✓Размещение оборудования в общих помещениях, куда имеют доступ работники подрядной организации, являющиеся потенциальными нарушителями в соотв. с моделью нарушителя; ✓Отсутствие документирования процедур контроля доступа и сопровождения оборудования, что может стать причиной сбоя (или отклонения от процедуры) и привести к ошибке персонала.	✓СКУД; ✓Правила контроля доступа к АСУ ТП; ✓Правила физической безопасности АСУ ТП; ✓Правила сопровождения АСУ ТП.
Угрозы осуществления НСД к АСУ ТП либо распространения вредоносных программ за счет подключения несанкционированных устройств к сети	✓ предполагаемый нарушитель, может подключить свое сетевое устройство путем разрыва кабеля... ✓В сети АСУ ТП отсутствуют механизмы, позволяющие фиксировать подключения к сети несанкционированных устройств; ✓Подключение несанкционированных устройств к корпоративной ЛВС не даст нарушителю значительных преимуществ в части проведения атак на АСУ ТП.	✓802.1x; ✓Правила безопасности сети АСУ ТП.

Непосредственной оценкой

	Эксп. 1	Эксп. 2		Эксп. M
Угр. 1				
Угр. 2				
…			p_{ij}	
Угр. N				

$$p_i = \sum_{j=1}^{M} \frac{1}{M} p_{ij}$$

Парным сравнением

Эксп. M	Угр. 1	Угр. 2		Угр. N
Угр. 1				
Угр. 2				
…			p^{M}_{ij}	
Угр. N				

$$p_i = \sum_{j=1}^{N} \sum_{m=1}^{M} \frac{1}{MN} p^{m}{}_{ij}$$

Эксп. 2	Угр. 1	Угр. 2		Угр. N
Угр. 1				
Угр. 2				
…			p^{2}_{ij}	
Угр. N				

Ранжированием

	Эксп. 1	Эксп. 2		Эксп. M
Угр. 1	2	1		5
Угр. 2	1	3		1
…				
Угр. N	5	2		2

Эксп. 1	Угр. 1	Угр. 2		Угр. N
Угр. 1				
Угр. 2				
…			p^{1}_{ij}	
Угр. N				

Шляхи мінімізації внутрішніх і зовнішніх загроз

Минимизация внутренних угроз

- Утечка/кража информации с ограниченным доступом (ДСП, КИ, КТ):
  - Категоризация информации компании; Организационные меры
  - Контроль почты, съемных носителей, интернет-трафика пользователей; DLP, proxy
  - Антивирусное ПО;
- Распространение вредоносного кода:
  - Обучение пользователей основам информационной безопасности; Организационные меры
  - Антивирусное ПО;
  - Обновление устаревшего оборудования и установка актуальных версий ОС/БД/ПО;
- Несанкционированный доступ к внутренним ресурсам компании:
  - Создание нормативной базы; Организационные меры
  - Сегментация сети; Firewall
  - Парольная политика; IDM
  - Устранение настроек по умолчанию; Compliance
  - Единая система управления учетными записями. IDM, SSO
- Несанкционированный перехват и модификация информации:
  - Контроль настроек сетевой безопасности; Compliance
  - Использование защищенных протоколов доступа; Compliance
  - Корпоративная инфраструктура PKI;
  - Обучение пользователей. Организационные меры
- Действия человеческого фактора, приводящие к остановке бизнес-критичных систем:
  - Внедрение контроля доступа привилегированных пользователей в системы по согласованию;
  - Внедрение систем контроля действий привилегированных пользователей;
  - Настройка журналирования событий. Сбор и корреляция. SIEM

Минимизация внешних угроз

- Конкурентная разведка:
  - Мониторинг публикуемой в Интернет информации компании;
  - Контроль за информацией, находящейся на серверах компании, доступных из Интернет.
- Распространение вредоносного кода:
  - Внедрение антиспам-систем в компании;
  - Контроль доступа в Интернет; Proxy, антивирус, контент-фильтрация
  - Антивирусная проверка электронной почты и веб-трафика;
  - Регулярное обновление антивирусного ПО на рабочих станциях пользователей.
- Несанкционированный доступ к ресурсам компании извне:
  - Создание безопасной архитектуры стыков с недоверенными сегментами; Квалифицированный аудит.
  - Правила фильтрации на стыках по принципу «разрешено только то, что разрешено»; Firewall
  - Применение парольной политики к системам в DMZ;
- Несанкционированный доступ к ресурсам компании извне:
  - Устранение настроек по умолчанию; Vulnerability management, Compliance
  - Контроль и обновление уязвимого ПО на серверах. Patch Management, Compliance
- Несанкционированный перехват и модификация информации:
  - Использование защищенных протоколов доступа;
  - Инфраструктура PKI;
  - Использование SSL-сертификатов, выданных доверенными CA на публичных ресурсах;
  - Обучение пользователей. Организационные меры
- Атаки на отказ в обслуживании (DoS, DDoS-атаки):
  - Своевременное обновление уязвимых версий ПО; Vulnerability management
  - Устранение настроек по умолчанию; Compliance
  - Внедрение систем защиты от DDoS-атак либо приобретение стороннего сервиса.

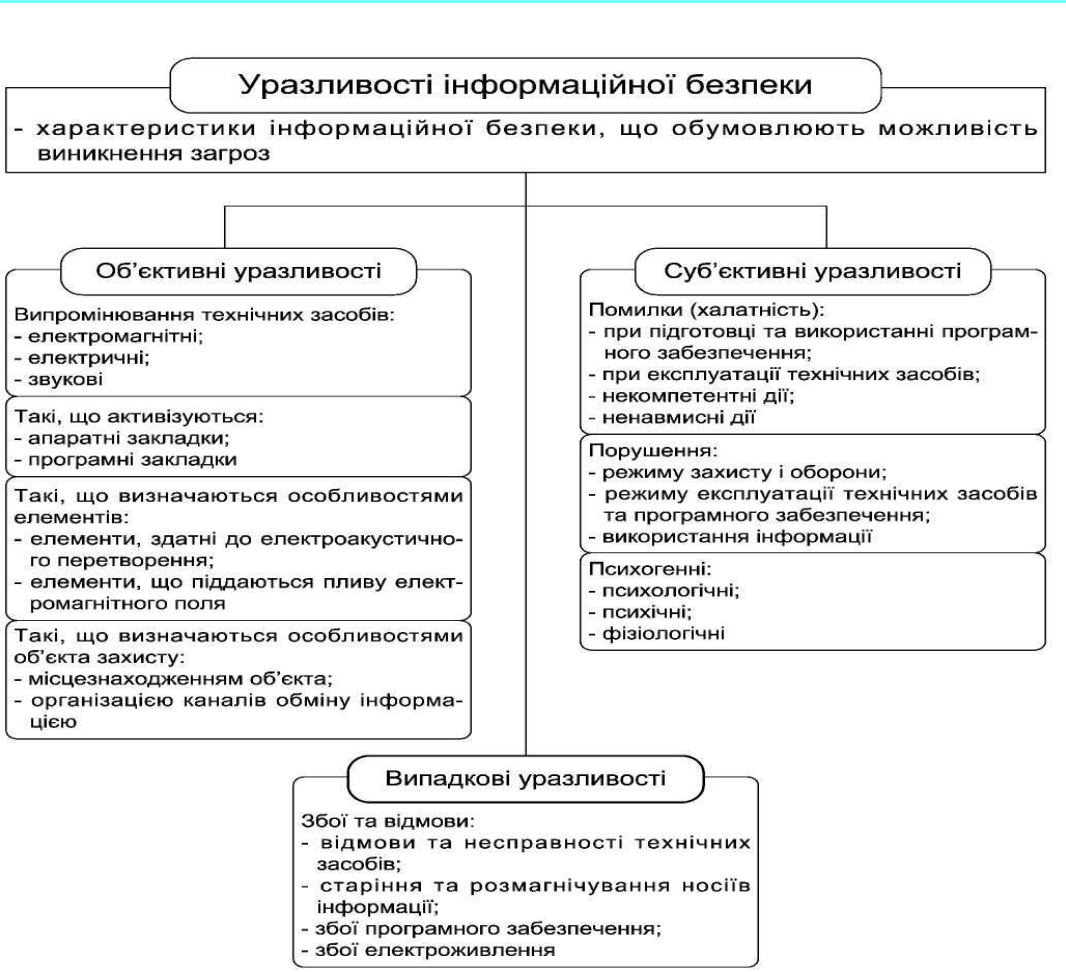
Класифікація уразливостей безпеки ІТС

Загрози, як можливі небезпечні прояви певної дії, спрямованої проти об'єкта захисту, реалізуються через *уразливості*.

Уразливість або слабкість (фактор) – *будь-яка характеристика або властивість ІС, використання якої порушником може привести до порушення безпеки інформації на об'єкті інформаційної діяльності.*

Уразливості, властиві ОІД, невіддільні від нього та обумовлюються недоліками процесу функціонування, властивостями архітектури ІС, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування інформаційної системи.
Усунення або суттєве послаблення уразливостей впливає на можливість реалізації загроз безпеці інформації.

Уразливості ІТС можуть бути об'єктивними, суб'єктивними або випадковими.



Об'єктивні уразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть суттєво послаблятися технічними та інженерно-технічними методами відбивання загроз безпеці інформації.

Суб'єктивні уразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.

Випадкові уразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливе тільки при проведення комплексу організаційних та інженерно-технічних заходів із протидії загрозам ІБ.

Класифікація уразливостей безпеки ІТС

За своєю суттю уразливості ІТС можна розділити на чотири типи:

- уразливості зумовлені відсутністю передбачених моделлю керування керуючих документів;
- уразливості зумовлені відсутністю передбачених моделлю керування керуючих процесів у випадку коли не виконуються передбачені моделлю керування керуючі дії;
- уразливості зумовлені відсутністю передбачених моделлю керування технічних рішень. Процедура повинна надавати можливість визначити задіяний у витоку інформації персонал та системи – відсутність засобів контролю витоку інформації;
- уразливості пов'язані з конкретним програмним забезпеченням та / або пристроєм.

Перелік уразливостей ІБ

Уразливості зумовлені відсутністю передбачених моделлю управління керуючих документів	Уразливості зумовлені відсутністю передбачених моделлю управління керуючих процесів	Уразливості зумовлені відсутністю передбачених моделлю управління технічних рішень	Уразливості пов'язані з конкретним програмним забезпеченням та / або пристроєм (у разі, якщо ПЗ є власною розробкою організації)
➢ відсутність політики парольного захисту; ➢ відсутність процедури поводження з носіями інформації; ➢ відсутність процедури захисту мережі	➢ відсутність моніторингу несправностей та помилок систем; ➢ відсутність періодичного перегляду існуючої класифікації інформації; ➢ не доведення до відома найманого персоналу, постачальників/ провайдерів / партнерів політики інформаційної безпеки	➢ відсутність захисту конфіденційної інформації під час передачі у формі приєднаних файлів; ➢ відсутність механізмів контролю дій систем ного адміністратора; ➢ відсутність механізмів обмеження доступу персоналу до інформації	➢ наявність прав привілейованих користувачів; ➢ можливість відключення режиму безпеки (від імені адміністратора); ➢ порушення послідовності виконання операцій з можливістю втручання в її хід на будь-якому етапі виконання (так звані «вікна»)

Базовий показник уразливості інформації

$$P_{ijk}^{(б)} = \prod_{l=1}^{5} [1-P_{ijkl}]^{5} = \prod_{l=1}^{5} [1-P_{ikl}^{(д)} * P_{ijl}^{(к)} * P_{ijkl}^{(н)} * P_{ijl}^{(и)}]$$

де $P_{ijkl} = P_{ikl}^{(д)} * P_{ijl}^{(к)} * P_{ijkl}^{(н)} * P_{ijl}^{(и)}$;

P_{ijkl} - імовірність несанкціонованого отримання інформації порушником k-ї категорії по j-ому каналу отримання інформації (КНОІ) в l-й зоне i-го структурного компонента ІС;

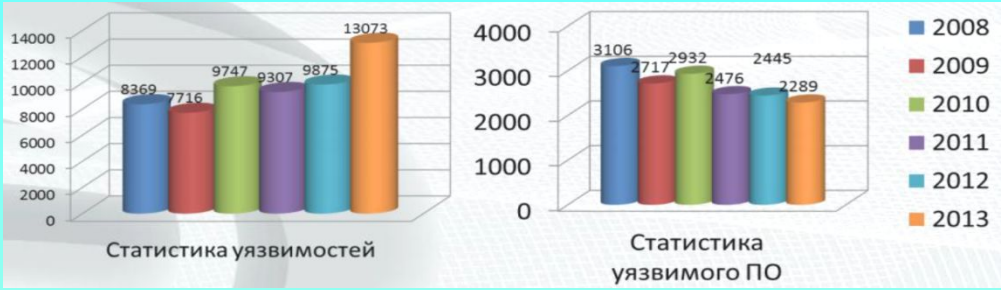
$P_{ikl}^{(д)}$ - імовірність доступа порушника k-ї категорії в l-у зону i-го компонента ІС;

$P_{ijl}^{(к)}$ – імовірність прояву j-ого КНОІ в l-й зоні i-го компонента ІС;

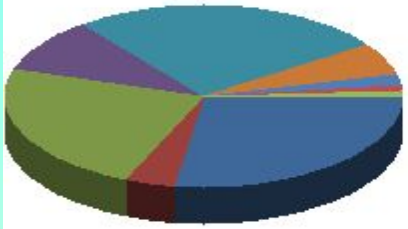
$P_{ijkl}^{(н)}$ - імовірність доступа порушника k-ї категорії до j-ого КНОІ в l-й зоні i-го компонента ІС за умови доступа порушника в зону;

$P_{ijl}^{(и)}$ - імовірність появи інформації, що підлягає захисту в j-м КНОІ в l-й зоні i-го компонента ІС в момент доступа туди порушника.

Статистика уразливостей ОС, ПЗ і додатків



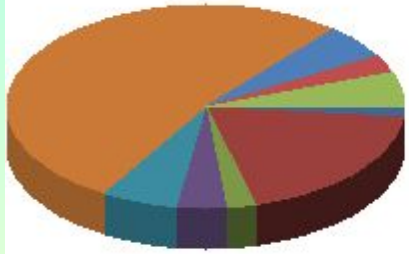
Типы уязвимостей в компонентах ОС



www.SecurityLab.ru

- Отказ в обслуживании (27.62%)
- Раскрытие важных данных (3.81%)
- Повышение привилегий (23.81%)
- Обход ограничений безопасности (9.52%)
- Компрометация системы (25.71%)
- Спуфинг атака (5.71%)
- Раскрытие системных данных (1.9%)
- Межсайтовый скриптинг (0.95%)
- Неавторизованное изменение данных (0.95%)

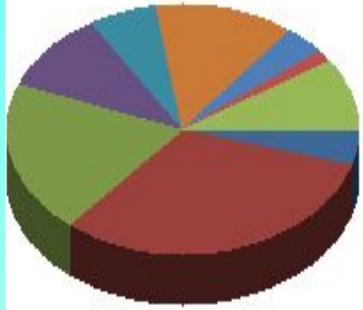
Типы уязвимостей в клиентском ПО



www.SecurityLab.ru

- Раскрытие системных данных (1.77%)
- Отказ в обслуживании (19.15%)
- Межсайтовый скриптинг (2.48%)
- Спуфинг атака (4.26%)
- Раскрытие важных данных (6.03%)
- Компрометация системы (52.48%)
- Обход ограничений безопасности (5.67%)
- Неавторизованное изменение данных (2.48%)
- Повышение привилегий (5.67%)

Типы уязвимостей в серверных приложениях



www.SecurityLab.ru

- Неавторизованное изменение данных (4.81%)
- Отказ в обслуживании (31.48%)
- Компрометация системы (20%)
- Межсайтовый скриптинг (10.37%)
- Повышение привилегий (5.93%)
- Обход ограничений безопасности (12.96%)
- Раскрытие системных данных (3.7%)
- Спуфинг атака (1.48%)
- Раскрытие важных данных (9.26%)

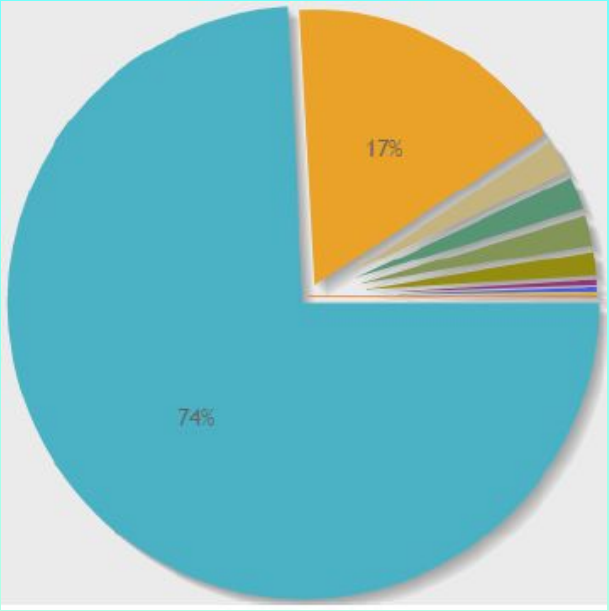
Какова бы не была квалификация сотрудников, человеческие возможности уже не позволяют самостоятельно обрабатывать гигабайты различной информации, связанной с безопасностью ИС!

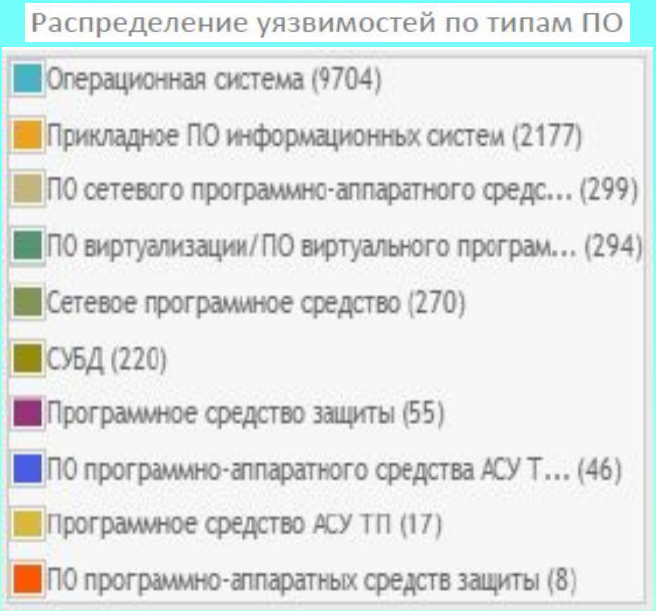
Рынок средств управления уязвимостями

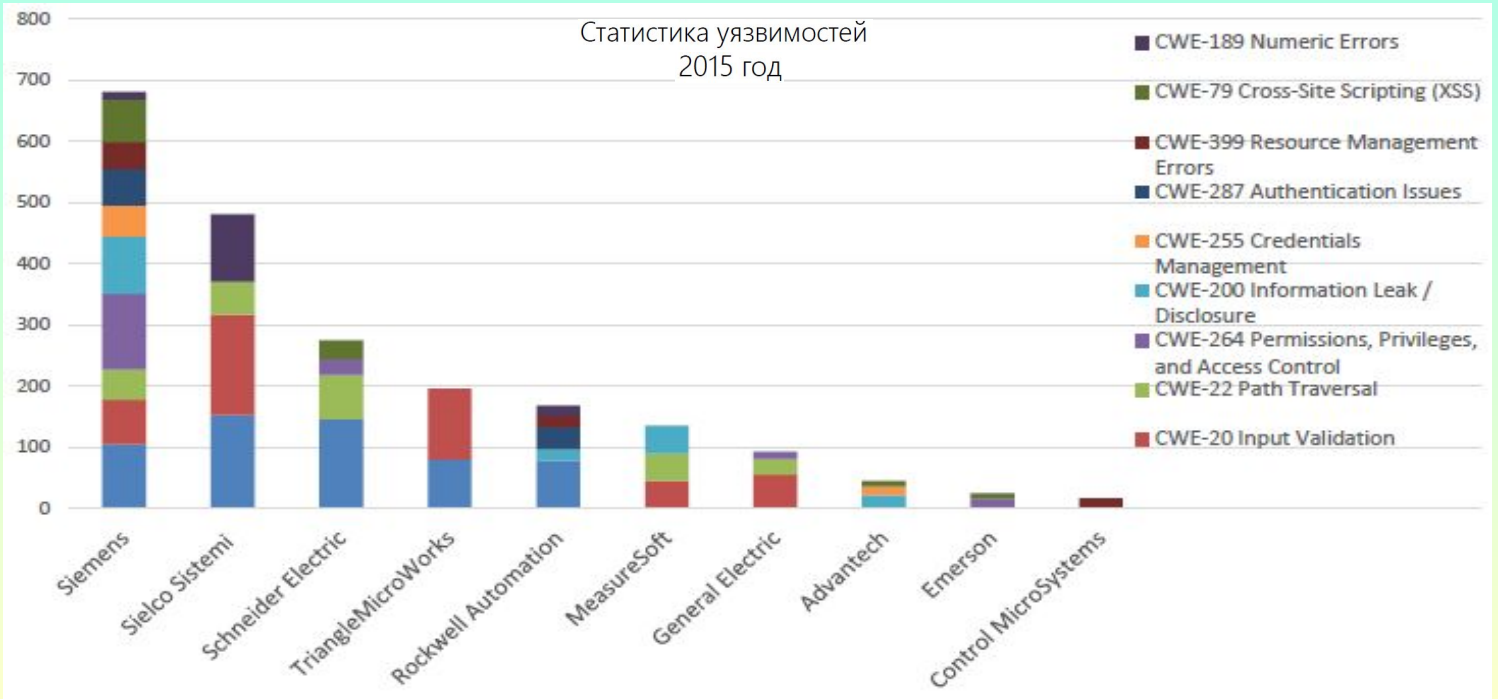
IDC: Worldwide Security and Vulnerability Management Revenue(segment Vulnerability assessment), $M

Как в ОС, так и в приложениях доминируют следующие уязвимости: отказ в обслуживании, компрометация системы и повышение привилегий.

Статистика уразливостей ОС, ПЗ і додатків







Висновки

1) У зв'язку із зростаючою роллю інформаційних ресурсів в житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема інформаційної та кібербезпеки вимагає до себе постійної і все більшої уваги.

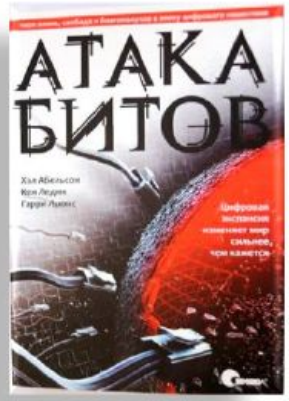
2) Системний характер впливу на ІКБ великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні даної проблеми.

3) Розуміючи ІКБ як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мету, а також інші умови і дії, що порушують безпеку.

4) Загрози ІКБ - це можливі дії або події, які можуть вести до порушень безпеки. Вони спрямовані на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації.

5) Одне з ключових понять в оцінці ефективності прояви загроз об'єкту ІКБ - збиток, що наноситься цьому об'єкту (підприємству) в результаті впливу загроз. За своєю суттю будь-який збиток, його визначення та оцінка мають яскраво виражену економічну основу. З позиції економічного підходу, загальний збиток ІКБ підприємства складається з двох складових частин: прямого і непрямого збитку. Прямий збиток ІКБ підприємства виникає внаслідок витоку конфіденційної інформації. Непрямий збиток - втрати, які несе підприємство у зв'язку з обмеженнями на поширення інформації, в установленому порядку віднесеної до категорії конфіденційної.

6) Опис збитку, що наноситься підприємству в результаті витоку конфіденційної інформації, грунтується на його кількісних і якісних показниках, які базуються на одному з принципів засекречування інформації (віднесення її до категорії конфіденційної) - принципі обгрунтованості. Він полягає у встановленні (шляхом експертних оцінок) доцільності засекречування конкретних відомостей, а також ймовірних наслідків цих дій, з урахуванням розв'язуваних підприємством задач і поставлених цілей.


АТАКА БИТОВ


Национальная платежная система
Бизнес-энциклопедия


Безопасность карточного бизнеса
Бизнес-энциклопедия
МФПА
CompuTel


Обеспечение информационной безопасности бизнеса
под редакцией А.П. Курило
IBM


Д.А. Мельников
ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО - ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ И СИСТЕМ
IDO PRESS


ВИКИ ЛИКС
КОМПРОМАТ НА РОССИЮ


ВИРТУАЛЬНЫЙ КРИМИНАЛ


Юрий Жуков
ОСНОВЫ ВЕБ-ХАКИНГА
НАПАДЕНИЕ И ЗАЩИТА
DVD


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ


ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


Крис Просис
Кевин Мандиа
Расследование компьютерных преступлений


СЕРИЯ «ВЫСШАЯ ШКОЛА»
А.Ю. Щербаков
СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
Теоретические основы
Практические аспекты


В.А. Сердюк
ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ
ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ИНФОРМАЦИОННЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ


Основы современной криптографии и стеганографии


Дж. Макнамара
СЕКРЕТЫ КОМПЬЮТЕРНОГО ШПИОНАЖА
ТАКТИКА И КОНТРМЕРЫ