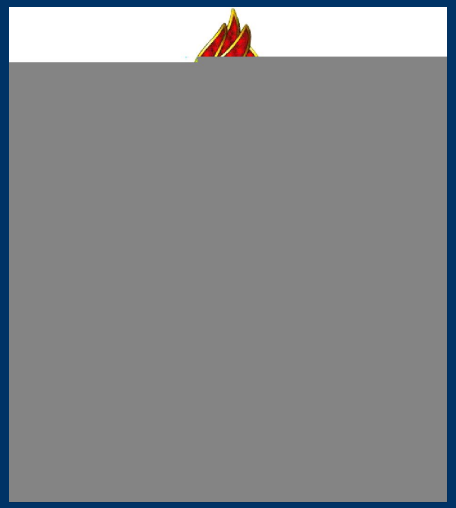
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
Імені ІВАНА ЧЕРНЯХОВСЬКОГО
КАФЕДРА ВІЙСЬКОВОЇ ПІДГОТОВКИ



НАВЧАЛЬНИЙ ЗБІР
ПРАКТИЧНЕ ЗАНЯТТЯ
З НАВЧАЛЬНОГО МОДУЛЯ ОЗБІ

КИЇВ - 2022

Тема 3. Основні положення забезпечення інформаційної та кібербезпеки

*Тема 3. Заняття 1.*Основи забезпечення інформаційної та кібербезпеки

1. Основні засади забезпечення інформаційної та кібербезпеки
2. Способи оцінки інформаційних ризиків.

Сучасні підходи до оцінки ризиків інформаційних технологій.

3. Сутність, зміст та цілі кібернавчань.

*Самостійна робота: в НУОУ та за межами:*Впливи інформаційних загроз на роботу посадових осіб органу управління.

ЛІТЕРАТУРА

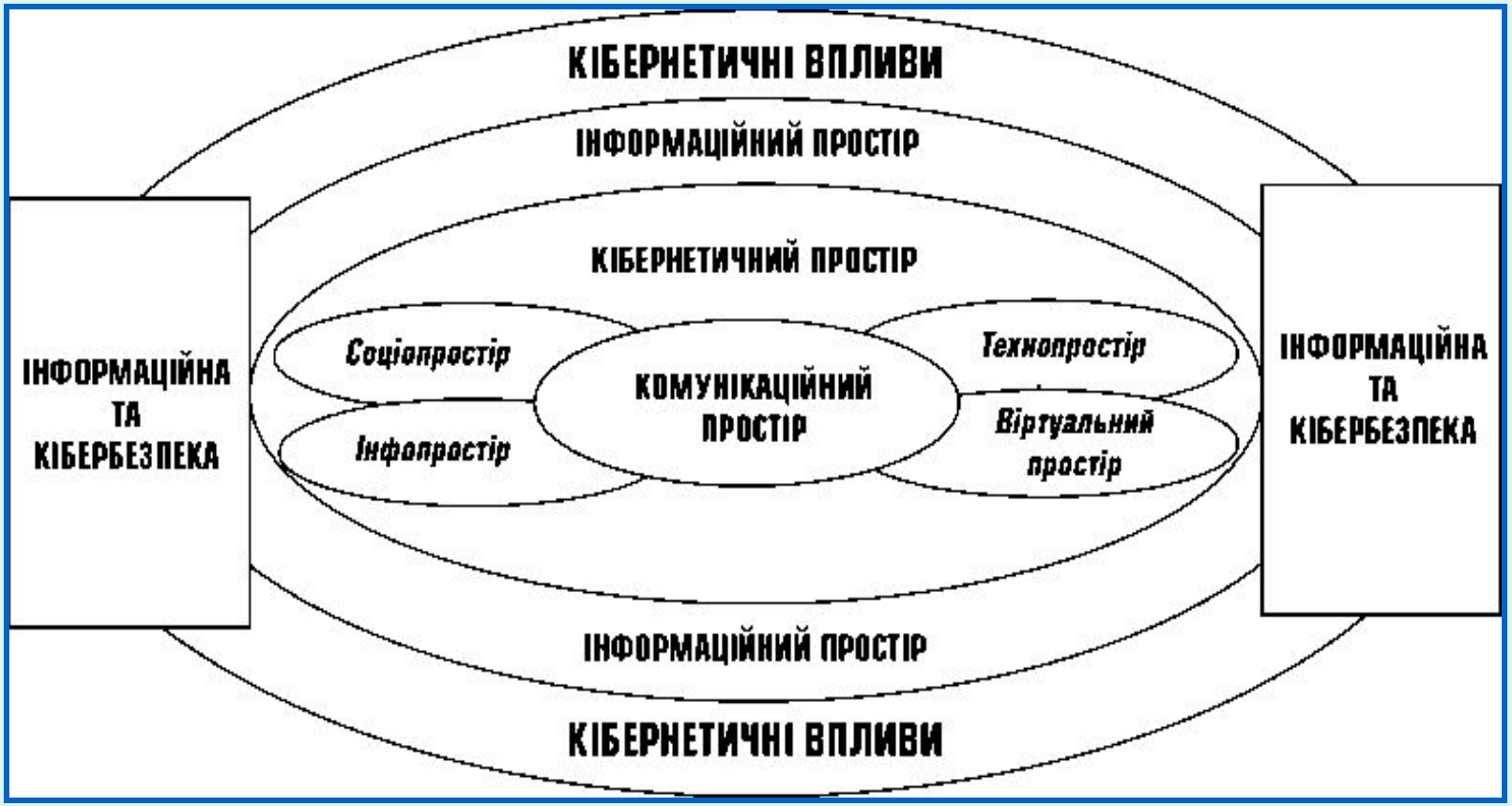
- 1. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 року (N 74/98-ВР).
- 2. . Статут внутрішньої служби ЗСУ від 1999 року із змінами.
- 3. Наказ МОУ від 17.09.2014 р. № 650 «Про затвердження Концепції інформатизації Міністерства оборони України».
- 4. Наказ МОУ від 01.04.2015 № 147 Положення про Реєстр електронних інформаційних ресурсів Міністерства оборони України.
- 5. П.П. Воробієнко та інші «Телекомунікаційні та інформаційні мережі», Київ 2010, 708 ст.
- 6. Закон України « Про захист інформації в інформаційно- телекомунікаційних системах» із змінами від 2014 року.

ЛІТЕРАТУРА

- Інформатизація штабів. Навчальний посібник. – К. Вид. НУОУ, 2012.
- Основи інформаційно-аналітичного забезпечення органів військового управління. Навчальний посібник. – К. Вид. НУОУ, 2014.
- Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. — [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, 2019. — 320 с.
- **ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА СОЦІОТЕХН АСПЕКТ.** Підручник за загальною редакцією д.т.н. проф. В. Б. Толубка. Київ ДУТ 2015

Аналізуючи умови функціонування військових органів управління, можна дійти висновку про те, що забезпечення конфіденційності, цілісності та доступності інформації стає складною задачею внаслідок впливу на ІТС і відповідно на роботу органу управління різноманітних факторів з боку зовнішнього середовища. Ці впливи об’єднуються поняттям **інформаційні та кіберзагрози**.

. Взаємозв'язок інформаційного та кіберпросторів



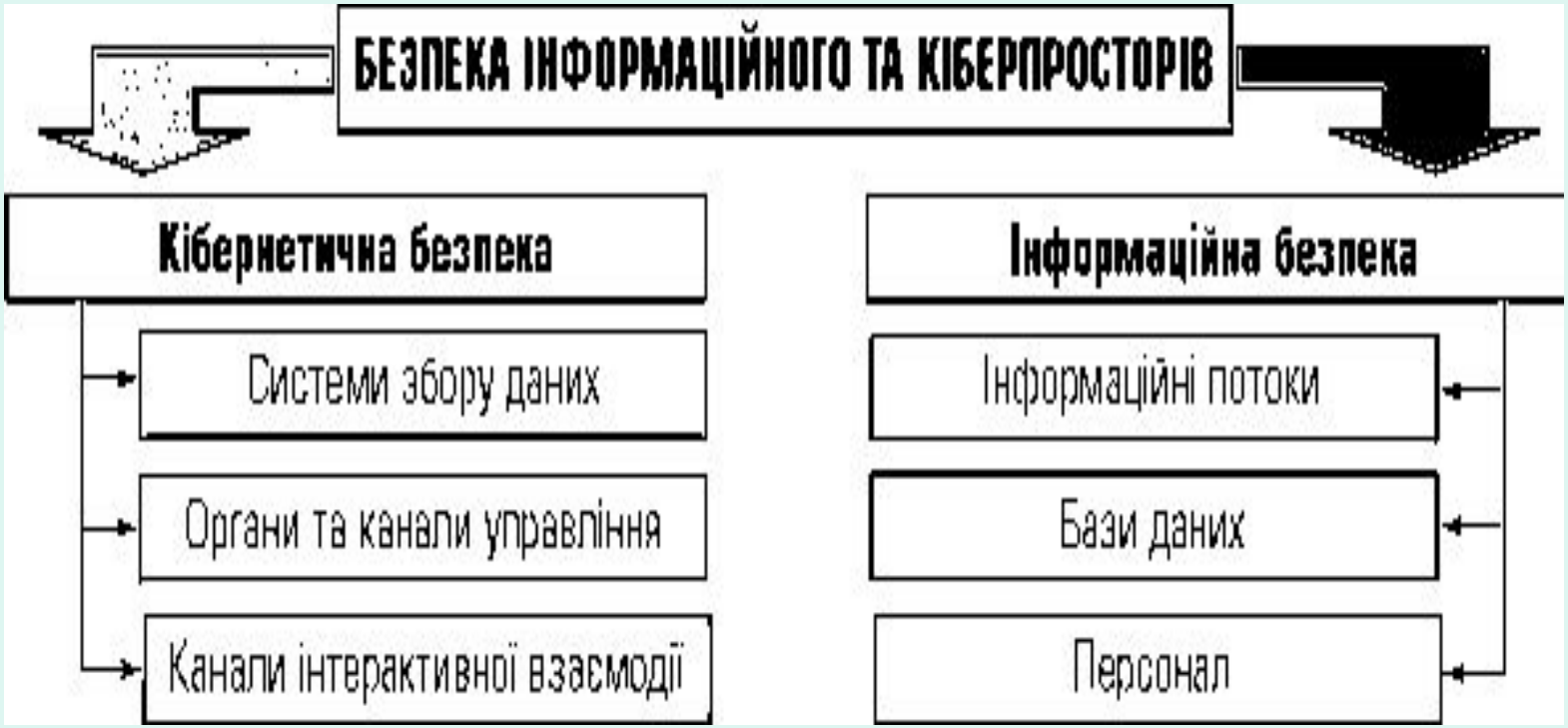
Загальна характеристика Кіберпростору

З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій **на кшталт проникнення в ІТС один одного**, блокування або виведення з ладу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сферами) і своєрідної сполученої ланки між такими поняттями, як інтернет і кібернетика, усе це, у свою чергу, дає змогу:

- **виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;**
- **схарактеризувати злочини, втручання і загрози, пов'язані з особливостями існування та передавання інформації;**
- **визначитись із можливими його дійовими особами;**
- **розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.**

.Дійові особи кіберпростору та їхній вплив на інформаційну і кібербезпеку

1.Основні засади забезпечення інформаційної та кібербезпеки



При цьому інформаційну безпеку (ІБ) у найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони

Забезпечення інформаційної безпеки ІТС

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії:

доступність — можливість за прийнятний час отримати певну інфор маційну послугу;

цілісність — актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання;

конфіденційність — захищеність від несанкціонованого ознайомлення

Головні загрози, які можуть спричинити порушення цих категорій, а також негативно вплинути на компоненти ІС, призвівши навіть до їх втрати, знищення чи збою функціонування, такі: ***розголошення інформації,*** **її *витік* або *несанкціонований доступ* до такої інформації**

Забезпечення інформаційної безпеки ІТС

Методи, завдяки яким цьому можна запобігти, забезпечивши відповідний рівень ІБ, доцільно класифікувати так:

- ***сервіси мережної безпеки*** (механізми захисту інформації, оброблюваної в розподілених обчислювальних системах і мережах);
- ***інженерно-технічні методи*** (мають на меті забезпечення захисту інформації від витоку по технічних каналах);
- ***правові та організаційні методи*** (створюють нормативну базу для організації різного роду діяльності, пов’язаної із забезпеченням ІБ);
- ***теоретичні методи забезпечення*** (розв’язують завдання формалізації різного роду процесів, пов’язаних із забезпеченням ІБ).

Основні методи забезпечення інформаційної безпеки

Складові кібернетичної безпеки ІТС

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам.

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ і ІТС

Забезпечення кібернетичної безпеки ІТС

Головні проблеми забезпечення кібернетичної безпеки постають з таких причин: відсутності чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави;

- дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки;
- залежності держави від програмних і технічних продуктів іноземного виробництва;
- відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки;
- дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів.

Сутність кібернетичної безпеки ІТС

КІБЕРНЕТИЧНА БЕЗПЕКА

АСПЕКТИ

Соціальний
Технічний
Інформаційний
Комунікаційний

СФЕРИ

Внутріщньополітична
Зовнішньополітична
Воєнна
Економічна
Соціальна
Екологічна
Науково-технічна

РІВНІ

Нормативно-правовий
Соціальний
Інфокомунікаційний
Соціотехнічний
Методичний

Критично важливі складові фізичної, інформаційної та кіберінфраструктури

Закон про основні засади забезпечення кібербезпеки України

Об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

Закон про основні засади забезпечення кібербезпеки України

Об’єктами кіберзахисту є:

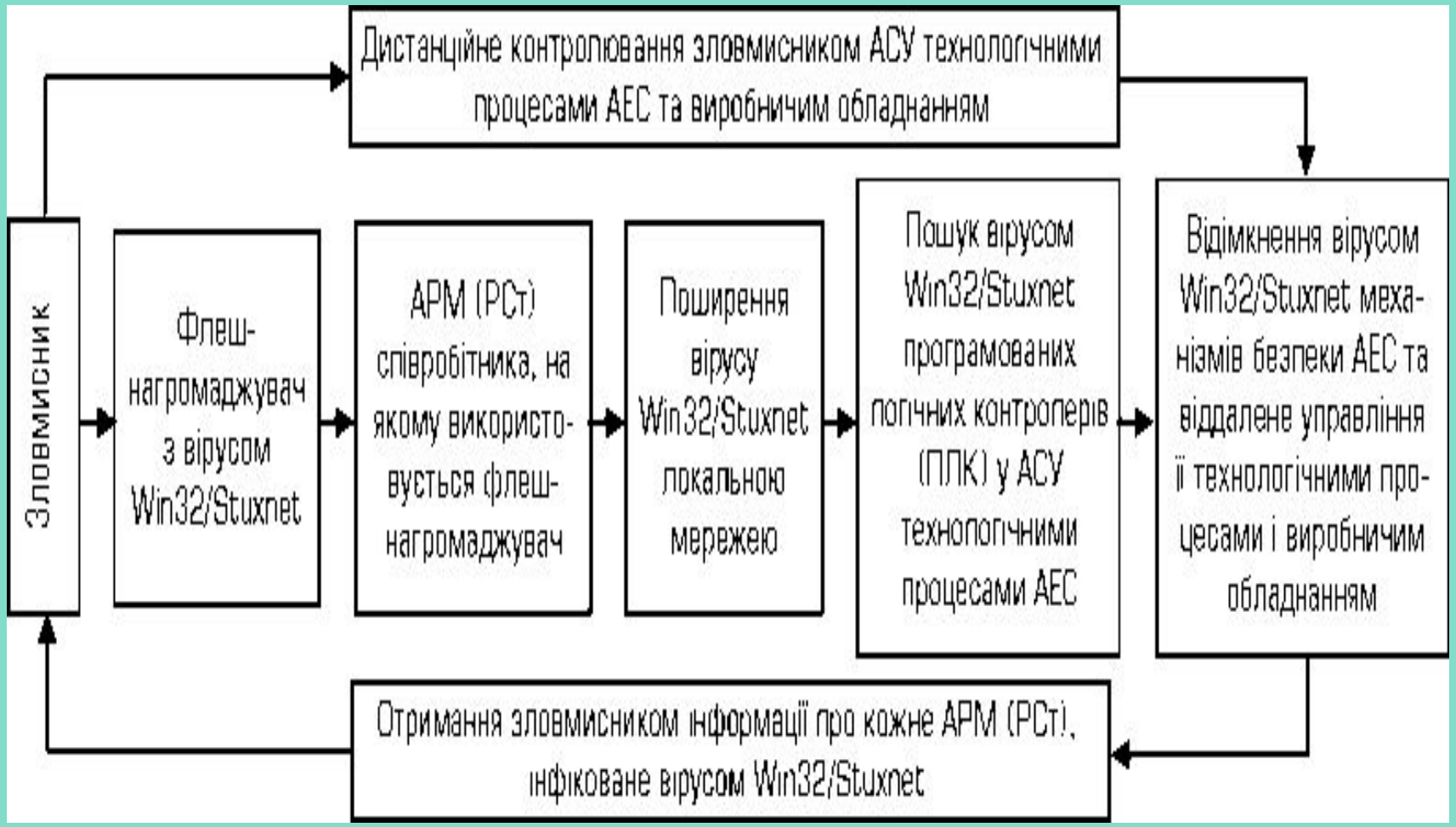
1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

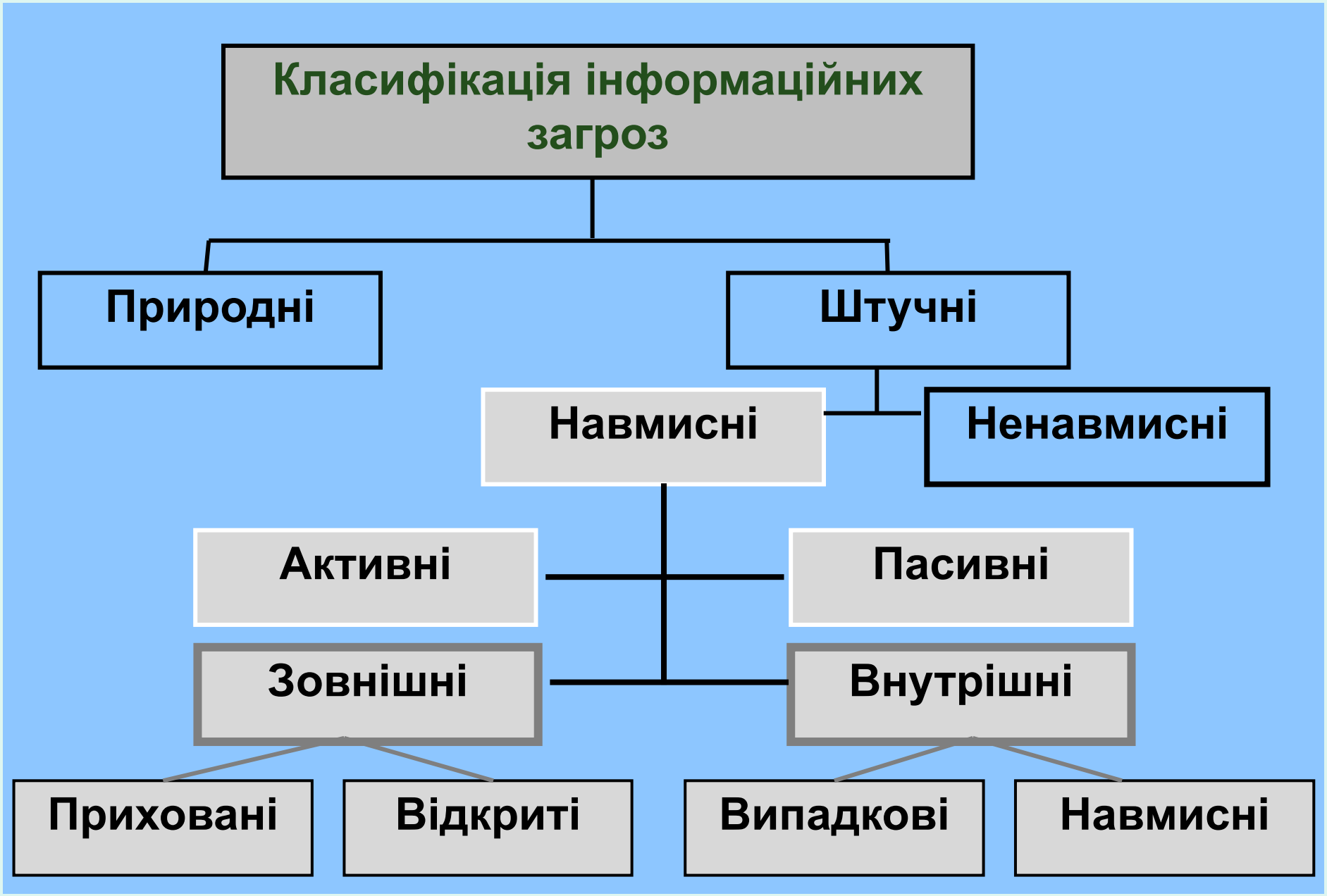
2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об’єктів критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Схема функціонування вірусу Win32/Stuxnet




Класифікація інформаційних загроз
Природні
Штучні
Навмисні
Ненавмисні
Активні
Пасивні
Зовнішні
Внутрішні
Приховані
Відкриті
Випадкові
Навмисні

Процес оцінки ризику оцінює ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності.
Потім вимірюється ефективність існуючих заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують курс дій для захисту активів. Існує безліч способів оцінки інформаційного ризику, розглянемо класифікацію існуючих методів і засобів оцінки інформаційних ризиків

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Вона включає у себе:

1) оцінку ймовірності загроз й уразливостей, які можливі;
2) розрахунок впливу, який може мати загроза на кожен актив;
3) визначення кількісної (вимірної) або якісної (описуваної) вартості ризику.

Треба взяти до уваги те, що ці три змінні майже завжди залежать одна від одної. В області інформаційної безпеки є зв'язок між вартістю активів, впливом і ймовірністю. Наприклад, більш імовірно, що хакер буде використовувати уразливість, яка викликає більший вплив, ніж уразливість з низьким рівнем впливу. Крім того, цінний актив має більшу імовірність компроментації, ніж марний. Таким чином, у цій області повинно прийматися до уваги більше, ніж просто випадкові дії. Необхідно брати до уваги, що за наявності достатнього 292 часу і рішучості, люди мають можливість обійти майже всі заходи безпеки. Вони можуть бути надзвичайно творчими, коли мотивовані. Таким чином, фактор мотивації повинен бути серйозно розглянутий в процесі оцінки безпеки інформаційного ризику

Загалом відомі три способи, за допомогою яких можна проводити оцінку інформаційних ризиків: 1) методи; 2) управляючі документи; 3) інструмент

1. **Методи.** Метод – це систематизована сукупність кроків, дій, які необхідно зробити для вирішення певної задачі або досягти поставленої мети, в даному випадку провести оцінку ризиків. Тобто метод – це покрокова інструкція плюс інструмент (програмний продукт) для проведення оцінки ризиків в організації
2. **Управляючі документи**. Крім методів оцінки ризиків використовують управляючі документи, де теоретично описуються і даються методичні вказівки процесу оцінки ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799
3. **Інструменти**. Крім методів та управляючих документів використовують інструменти для оцінки ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами, існуючими без методики з покроковою інструкцією, є: Cobra, RiskWatch.

Всі методи оцінки ризику можна поділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішані).

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. Мета полягає в тому, щоб обчислити числові значення для кожного з компонентів, зібраних у ході оцінки ризиків та аналізу витрат і переваг. ISAMM (виробник: Бельгія)

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як "низький, середній, високий", "не важливо, важливо, дуже важливо або "за шкалою від 1 до 10". Якісна модель оцінює дії й імовірності виявлених ризиків швидким й економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику та можуть послужити основою для цілеспрямованої кількісної оцінки.

Mehari (виробник: Франція). EBIOS (виробник: Франція)

CRAMM (виробник: Великобританія) – змішаний метод, який досить складно використовувати без CRAMM інструмента. В інструмента така сама назва, як і у методу – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектору. Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких є можливість економічного обґрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками дозволяє, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат. Має допоміжні програмні інструменти.

До сильних сторін методу CRAMM відноситься наступне:

- CRAMM є добре структурованим і широко випробуваним методом аналізу ризиків, що дозволяє отримувати реальні практичні результати;
- програмний інструментарій CRAMM може використовуватися на всіх стадіях проведення аудиту безпеки інформаційної системи (ІС);
- в основі програмного продукту лежить досить об'ємна база знань з контрзаходів в області інформаційної безпеки, що базується на рекомендаціях стандарту BS 7799;
- гнучкість і універсальність методу CRAMM дозволяє використати його для аудиту ІС будь-якого рівня складності і призначення;
- CRAMM можна використати як інструмент для розробки плану безперервності бізнесу і політики інформаційної безпеки організації;
- CRAMM може використовуватися як засіб документування механізмів безпеки ІС

До недоліків методу CRAMM можна віднести наступне:

- використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;
- CRAMM набагато більшою мірою підходить для аудиту вже існуючих ІС, таких, що знаходяться на стадії експлуатації, ніж для ІС, що знаходяться на стадії розробки;
- аудит за методом CRAMM – процес досить трудомісткий і може потребувати місяців безперервної роботи аудитора;
- програмний інструментарій CRAMM генерує значну кількість паперової документації, яка не завжди виявляється корисною на практиці;
- CRAMM не дозволяє створювати власні шаблони звітів або модифікувати наявні;
- можливість внесення доповнень у базу знань CRAMM не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації.

Cobra (виробник: Великобританія) – програмний інструмент, який дозволяє проводити оцінку ризиків у галузі безпеки. Він оцінює відносну важливість усіх загроз й уразливостей, генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці. Крім того, конкретний район або питання може бути розглянуте "самостійно", без будь-яких наслідків для організації.

Управління ризиками кібербезпеки є одним із компонентів управління ризиками установи й особливо важливо в організаціях і підприємствах, які значною мірою залежать від мереж і систем інформаційних технологій (ІТ) для їх діяльності.

Управління ризиками – це процес виявлення уразливостей і загроз інформаційних ресурсів, що використовуються організацією для досягнення цілей і прийняття рішень про те, які контрзаходи, якщо такі є, повинні приймати по зниженню ризику до прийнятного рівня на основі цінності інформаційного ресурсу для організації.

Основні підходи до управління ризиками інформаційних технологій ґрунтуються на:

- стандарті управління та аудиту інформаційних технологій Cobit v.4.1;
- настановах по управлінню ризиками в інформаційних технологіях NIST 800-30;
- настановах по управлінню ризиками ISO 3100 (вводяться);
- стандарті управління інформаційною безпекою ISO 27005;
- стандарті управління ризиками AS/NZS 4360:2005.

Методика оцінки ризиків NIST Стандарт США NIST 800-30 “Керівництво з інформаційними ризиками ІТсистем” – керівництво з аналізу та управління ризиками був розроблений Лабораторією інформаційної технології (ITL) Національного інституту стандартів і технології (NIST) США і надані рекомендації в керівництві з аналізу та управління ризиками. Відповідно до NIST SP 800-30 Методологія оцінки ризику охоплює дев'ять основних етапів : характеристика системи; ідентифікація загроз; ідентифікація уразливості; аналіз заходів захисту; визначення правдоподібності; аналіз впливу; визначення ризиків; рекомендації до заходів захисту; документація результатів. У кожному етапі на основі логіки зв'язків з певної вхідної інформації виходить вихідна

3. Сутність, зміст та цілі кібернавчань.

Проблеми підготовки фахівців у сфері кібербезпеки актуальні для багатьох країн світу. Першочерговий інтерес викликає досвід у цій галузі США, КНР та країн НАТО.

Напрями, зміст та обсяги підготовки фахівців кібербезпеки у цих країнах визначаються:

- рівнем та напрямами розвитку національних Збройних Сил;
- ступенем їх уразливості у кіберпросторі;
- ступенем розуміння органами державного управління загроз кібербезпеці;
- заходами нормативно-правового та організаційного забезпечення системи кібербезпеки;
- визначеними завданнями кадрового забезпечення розгорнутих і перспективних систем кібербезпеки, а також можливостями систем військової і цивільної освіти кожної із визначених країн

Сутність, зміст та цілі кібернавчань.

Найбільш потужна система підготовки військових фахівців кібербезпеки створена у США для кадрового забезпечення Кіберкомандування, деяких інших компонентів ЗС США, у тому числі підрозділів сил спеціальних операцій та операцій бойового забезпечення, а також Агентства національної безпеки (АНБ).

Крім США підготовку військових фахівців у сфері кібербезпеки здійснюють країни-члени НАТО. Так, офіцерський склад ЗС країн НАТО має можливість проходити перепідготовку і підвищувати кваліфікацію на різних спеціалізованих курсах у рамках Альянсу, зокрема, на курсах психологічних операцій і в роботі з цивільним населенням для командного складу НАТО при навчальному центрі британської військової розвідки в м. Чиксендзі (Великобританія), курсах НАТО в м. Обераммергау (Німеччина), в Об'єднаному центрі передових технологій з кібероборони НАТО (англ. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) у м. Таллінн (Естонія) тощо

Сутність, зміст та цілі кібернавчань.

На окрему увагу заслуговує такий вид підготовки сил кібербезпеки, як проведення навчань та тренувань різного рівня. Показовою у цьому напряму є діяльність, спрямована на злагодження підрозділів кібероперацій збройних сил США та НАТО. Так, у США заходи оперативної та бойової підготовки ЗС із залученням сил кібербезпеки спрямовані окрім іншого на практичне відпрацювання питань їх переведення з мирного у воєнний стан та організацію дій згідно з планами воєнного часу із врахуванням особливостей їх підпорядкування (сили кібербезпеки входять до складу Кіберкомандувань видів ЗС США і Морської піхоти, які оперативно підпорядковані Кіберкомандуванню). На таких навчаннях, як правило, моделюються різні стани воєнно-стратегічної обстановки і у подальшому командно-штабним методом відпрацьовуються варіанти залучення сил кібероборони на різних фазах воєнних конфліктів.

Сутність, зміст та цілі кібернавчань.

В основу таких заходів покладено вирішення наступних задач:

- перевірка можливості реалізації різних способів боротьби у кіберпросторі в умовах автоматизації управління Збройними Силами та активної протидії зі сторони противника;
- моделювання кібероперацій для вивчення способів впливу на інформації, об’єкти мережної інфраструктури й органи управління противника, оцінки здійснюваних ефектів і наслідків, як для противника, так і для США та їх союзників;
- оцінка бойових можливостей сил кібероборони і перспектив їх інтеграції з можливостями сил і засобів збройної боротьби на суходолі, у морі, повітрі та навколоземному космічному просторі для досягнення синергетичного ефекту при проведенні усього спектра військових операцій

Сутність, зміст та цілі кібернавчань.

Аналіз практичних заходів показує, що на даний час головна увага приділяється підвищенню ефективності захисту глобальної інформаційної інфраструктури (GII, Global information infrastructure) при різноманітних сценаріях кібернападів з боку агресорів. Крім того, зусилля спрямовані на інтеграцію кібероперацій у плани проведення інформаційних та повітрянокосмічних операцій, а також на оцінку можливостей проведення самостійних заходів для досягнення стратегічних цілей

Вимоги до обробки та передачі службової інформації.

Відповідно до вимог частини другої статті 6 Закону «Про доступ до публічної інформації»до службової належить інформація:

- що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, **у сфері оборони країни, яку не віднесено до державної таємниці.**

Вимоги до обробки та передачі службової інформації.

Документам, що містять службову інформацію, присвоюється гриф «Для службового користування». Доступ до таких документів надається відповідно до частини другої статті 6 Закону, згідно з якою обмеження доступу до інформації здійснюється при дотриманні таких вимог:

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
- розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Віднесення інформації до службової інформації здійснюється на підставі рішення експертної комісії МОУ.

Вимоги до обробки та передачі службової інформації.

Перелік відомостей, що становлять службову інформацію з обмеженим доступом у Міністерстві, розглядається експертною комісією і затверджується наказом МОУ.

Відповідальність за організацію обліку, обробку, зберігання, передачу та використання документів та інших матеріальних носіїв, які містять відомості, що становлять службову інформацію, та їх копій у структурних підрозділах Міністерства, а також контроль за дотриманням нормативних вимог покладаються на керівників структурних підрозділів.

Передача документів, які містять відомості, що становлять службову інформацію, від одного структурного підрозділу до іншого здійснюється з обов'язковою відміткою у спеціальному журналі, та в облікових формах структурних підрозділів загального діловодства (для вхідних документів).

Вимоги до обробки та передачі службової інформації.

Облік електронних носіїв інформації з грифом «Для службового користування» ведеться в журналах за визначенною формою.

Розмноження документів з грифом «Для службового користування» на розмножувальних апаратах здійснюється з дозволу та під контролем визначених керівників.

Обробка (друкування) документів з грифом «Для службового користування» з використанням інформаційно-телекомунікаційної системи здійснюється тільки після створення в ній комплексної системи захисту інформації та підтвердження відповідності створеної системи вимогам нормативних документів (за наявності атестата відповідності комплексної системи захисту інформації).

Вимоги до обробки та передачі службової інформації.

Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;
- результатів виконання користувачем операцій з обробки інформації;
- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;
- результатів перевірки цілісності засобів захисту інформації.

Вимоги до обробки та передачі службової інформації.

-Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

-Передача службової інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

-Порядок підключення систем, в яких обробляється службова інформація до глобальних мереж передачі даних визначається законодавством.

Основні терміни в сфері захисту інформації :

- **блокування інформації в системі** - дії, внаслідок яких унеможливлюється доступ до інформації в системі;
- **виток інформації** - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;
- **володілець інформації** - фізична або юридична особа, якій належать права на інформацію;
- **власник системи** - фізична або юридична особа, якій належить право власності на систему;
- **доступ до інформації в системі** - отримання користувачем можливості обробляти інформацію в системі;
- **захист інформації в системі** - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;
- **знищення інформації в системі** - дії, внаслідок яких інформація в системі зникає;

Законодавство щодо захисту інформації в ІТС

- **інформаційна система** - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;
- **інформаційно-телекомунікаційна система** – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;
- **комплексна система захисту інформації** - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;
- **користувач інформації в системі** – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;
- **криптографічний захист інформації** - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

Законодавство щодо захисту інформації в ІТС

- **обробка інформації в системі** - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;
- **порушення цілісності інформації в системі** – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;
- **порядок доступу до інформації в системі** - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;
- **телекомунікаційна система** - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;
- **технічний захист інформації** - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Об'єкти захисту в системі .

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

- володільці інформації;
- власники системи;
- користувачі;
- спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

Законодавство щодо захисту інформації в ІТС

В розвиток положень законодавства захист інформації в Збройних силах України організується на підставі наказів Міністра оборони, Начальника Генерального штабу – Головнокомандувача Збройних Сил України. На основі цих наказів здійснюється політика безпеки інформації в органі управління: сукупність документованих правил, процедур, практичних прийомів або керуючих принципів в галузі безпеки інформації та кібербезпеки, на основі яких відбувається діяльність органу управління.

Політика визначає основні напрямки захисту інформації:

- визначення інформаційних та технічних ресурсів, які підлягають захисту;
- виявлення повної множини потенційно можливих загроз та каналів витоку інформації;
- проведення оцінки вразливості та ризиків інформації за наявності множини загроз та каналів витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та обґрунтування їх характеристик;
- впровадження та організація використання обраних заходів захисту інформації;
- здійснення контролю цілісності та управління системою захисту.

До основних організаційних заходів можна віднести:

1. Організацію режиму та охорони, що виключає можливість проникнення на територію і в приміщення сторонніх осіб.
2. Організацію роботи із посадовими особами: підбір та розставлення персоналу, їх вивчення, навчання правилам роботи, ознайомлення з мірою відповідальності за порушення правил захисту інформації.
3. Організацію роботи з документами та документованою інформацією, їх розробку, використання, облік, збереження та знищення.
4. Організацію використання технічних засобів збору, обробки, накопичення та збереження конфіденційної інформації.
5. Організацію роботи з аналізу внутрішніх та зовнішніх загроз конфіденційній інформації та відпрацювання заходів з її захисту.
6. Організацію роботи з проведення систематичного контролю за роботою особового складу з інформацією, порядком обліку, збереження та знищення документів та технічних носіїв.

Заходи щодо захисту інформації в ІТС

Категорування ПК

Здійснюється спецпідрозділами до початку експлуатації ПК в обовязковому порядку за замовленнями. Без цього експлуатація ПК заборонена.

Резервування

1. Джерел електроживлення
2. Головних елементів ЛОМ (серверов, каналів передачі даних та ін.)
3. Створення дисків-дублерів для копіювання робочої інформації в мережі.
4. Архівірування файлів та збереження їх на автономних носіях (створенні архівних бібліотек)

Захист від радіотехнічної розвідки

1. Екранування приміщень, елементів мережі та ПК
2. Встановлення апаратури постановки активних перешкод
3. Захист каналів передачі даних
4. Встановлення електророзв'язок на енергомережах, каналах передачі даних.
5. Встановлення спеціального порядку роботи ПК в особливих умовах (активізація дій противника).

Заходи щодо захисту інформації в ІТС

Режимні заходи

1. Обмеження на вмикання енергопостачання в неробочий час.
2. Встановлення системи паролів на включення ПК.
3. Встановлення сигнально-контролюючої апаратурыи для груп адміністрування.

Розмежування доступу на ПК

1. Організація ідентифікації та аутентифікації користувачів.
2. Встановлення системи паролів для колективної роботи на ПК та розмежування доступу до нього.
3. Захист основних параметрів ОС, прикладних програм та кінцевих пристроїв від навмисної модифікації.
4. Безумовне копіювання робочої інформації на автономних носіях.
5. Захист файлів при архівації.

Заходи щодо захисту інформації в ІТС

Розмежування доступу до ресурсів ІТС

1. Вибір топології мережі відповідно до виконуваних завдань та вимог максимальної безпеки ресурсів.
2. Кваліфіковане адміністрування мережі та захист системи протоколів.
3. Встановлення системи ідентифікації та аутентифікації користувачів з встановленням контролю за використанням виділених ресурсів.
4. Встановлення обмежень на зовнішній вихід з ЛОМ та вхід до неї.

Кодування інформації

1. Використання криптостійких програм кодування.
2. Своєчасна зміна ключів кодування та організація їх збереження.
3. Виключення повторного використання ключів та передачі їх стороннім особам.

Закон про основні засади забезпечення кібербезпеки України

Кіберпростір – середовище існування та розповсюдження інформації, яке утворюється.

Кіберінфраструктура –єдність інформаційно-телекомунікаційних систем, центрів накопичення, збереження обробки та розповсюдження інформації на машинних носіях, засобів захисту інформації, а також організаційних структур, що забезпечують їх функціонування.

Кіберзброя – різновид інформаційної зброї, головним елементом якого є інформація та інформаційні технології, способи та засоби інформаційного впливу та захисту від нього, які призначені для ведення інформаційної боротьби у кіберпросторі.

Кібератака – цілеспрямований вплив на елементи ІТС з метою порушення доступності, цілісності та конфіденційності інформації, перешкоджання роботі та виведенню з ладу ІТС або її окремих елементів, основна форма інформаційної боротьби в кіберпросторі.

Кібербезпека – захищеність ІТС від навмисних та ненавмисних загроз їх функціонуванню.

Кіберзахист – сукупність правових, організаційних, технічних та технологічних заходів щодо передбачення та нейтралізації загроз функціонуванню обєктів кіберінфраструктури

Закон про основні засади забезпечення кібербезпеки України

кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;

критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури;

критично важливі об'єкти інфраструктури (далі - об'єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов' язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

ЗАГАЛЬНІ ВИСНОВКИ

Наявність у органі управління ретельно спланованої та відповідним чином організованої системи захисту інформації є необхідною умовою надійного забезпечення потрібними даними та командами військ.

Обмеження доступу до інформації має здійснюватись комплексом заходів:

- **режимного характеру;**
- **програмно-організаційними обмеженнями (адміністрування);**
- **спеціального призначення (зміна паролів, системи криптографування, поновлення мережевих програмних засобів фільтрації доступу в мережу та ін.).**

1. Дати визначення поняття «безпека інформація».
2. Навести приклади інформаційних загроз.
3. Навести приклади активних загроз.
4. Пояснити поняття «захист інформації».
5.Визначити основні напрями захисту інформації.
6.Визначитиорганізаційні заходи щодо захисту інформації.

Завдання на самостійну підготовку:

Законспектувати основні положення Стратегії кібербезпеки України.

ФАКУЛЬТЕТ ПІДГОТОВКИ ОФІЦЕРІВ ЗАПАСУ

За Україну, за її волю, за честь і славу, за народ!

ТЕЛЕФОНИ ДЛЯ ДОВІДОК:
271-09-72, 271-09-71