**1 Основи кібербезпеки**

**1.1 Поняття кіберпростору та інформаційного простору.**

Кіберпростір: Це віртуальне середовище, що включає в себе всі комп'ютерні системи, мережі, програмне забезпечення та дані, які з'єднані через Інтернет. Кіберпростір об'єднує людей, компанії, установи та держави, дозволяючи їм обмінюватися інформацією та взаємодіяти в онлайн-середовищі.

Інформаційний простір: Це концептуальне середовище, що включає в себе всі форми і типи інформації, які існують у світі. Це можуть бути дані, знання, медіа, документи, комунікації тощо. Інформаційний простір визначається не тільки обсягом і типами інформації, але і доступністю, якістю та способами обробки та розповсюдження.

**1.2 Інформаційна безпека як сфера національної безпеки України, безпеки підприємства/установи,**

**особистої безпеки.**

Інформаційна безпека є критично важливою для різних сфер життя, включаючи національну безпеку, безпеку підприємств/установ та особисту безпеку.

1. Національна безпека України: Інформаційна безпека є ключовим компонентом національної безпеки. Забезпечення захисту інформації від кіберзагроз, шпигунства та інших атак є критично важливим для збереження суверенітету, стабільності та розвитку держави.

2. Безпека підприємства/установи: Інформаційна безпека для підприємств та установ охоплює заходи щодо захисту конфіденційної інформації, клієнтських даних, фінансових операцій та інших важливих ресурсів. Це включає в себе застосування технологічних засобів захисту, навчання персоналу та розробку політик безпеки.

3. Особиста безпека: Інформаційна безпека на особистому рівні стосується захисту особистих даних, фінансової інформації, а також забезпечення безпеки в інтернеті. Це включає в себе застосування сильних паролів, уникання небезпечних веб-сайтів та електронних шахрайств, а також усвідомлення ризиків онлайн-діяльності.

**1.3 Поняття кібербезпеки, захисту інформації та кіберзахисту.**

Кібербезпека, захист інформації та кіберзахист є тісно пов'язаними поняттями, які спрямовані на захист інформації та комп'ютерних систем від кіберзагроз. Ось що означають ці терміни:

1. Кібербезпека: Це практика захисту комп'ютерних систем, мереж і даних від несанкціонованого доступу, зловживання, втрати чи пошкодження. Кібербезпека включає в себе різноманітні технології, процедури та стратегії, які застосовуються для запобігання кібератак і забезпечення безпеки цифрового середовища.

2. Захист інформації: Це процес застосування технічних, організаційних і фізичних заходів для забезпечення конфіденційності, цілісності та доступності інформації. Захист інформації включає в себе шифрування даних, встановлення прав доступу, резервне копіювання інформації та інші заходи для захисту важливої інформації від несанкціонованого доступу.

3. Кіберзахист: Це сукупність заходів і технологій, спрямованих на запобігання, виявлення та відновлення від кібератак. Кіберзахист включає в себе застосування програмного та апаратного забезпечення для виявлення та блокування шкідливих програм і активностей, моніторинг мережі для виявлення аномальної поведінки, а також планування та реалізацію заходів реагування на кіберінциденти.

**1.4 Види захисту інформації: технічний, Інженерний криптографічний, організаційний.**

Види захисту інформації включають технічний, інженерний та організаційний підходи:

1. Технічний захист: Це використання технологічних засобів та механізмів для захисту інформації. Це можуть бути шифрування даних, використання брандмауерів та антивірусного програмного забезпечення, впровадження сильних паролів та інші технічні засоби для запобігання несанкціонованому доступу та зловживанням.

2. Інженерний захист: Це застосування інженерних та фізичних заходів для захисту інформації. Це можуть бути біометричні системи доступу, контроль доступу до приміщень та обладнання для захисту обладнання від фізичного доступу.

3. Організаційний захист: Це встановлення політик, процедур та правил, що стосуються використання інформації та управління доступом до неї. Це може включати навчання персоналу щодо безпеки інформації, встановлення прав доступу до даних на основі ролей та відповідальностей, а також контроль за дотриманням внутрішніх політик безпеки.

**1.5 Поняття конфіденційності, цілісності, доступності.**

Поняття конфіденційності, цілісності та доступності (відомі як CIA трикутник) є ключовими аспектами інформаційної безпеки:

1. Конфіденційність: Це забезпечення того, що інформація доступна лише тим, хто має на це право. Іншими словами, конфіденційність гарантує, що інформація залишається виключно для обмеженого кола осіб, які мають відповідні дозволи або права доступу.

2. Цілісність: Це забезпечення того, що інформація залишається непорушною, недоторканою та незмінною протягом всього її життєвого циклу. Іншими словами, цілісність гарантує, що інформація не піддавалася неправомірним або несанкціонованим змінам, модифікаціям або втратам.

3. Доступність: Це забезпечення того, що інформація доступна тим, хто має право на її отримання, коли вони цього потребують. Доступність означає, що інформація доступна у відповідний час та місце для виконання відповідних завдань і функцій.

**1.6 Принципи кібербезпеки.**

Принципи кібербезпеки є фундаментальними правилами та керівними принципами, які спрямовують стратегії та практики забезпечення безпеки в інформаційній сфері. Основні принципи включають:

1. Принцип найменшого привілею: Надавати доступ лише тим користувачам, яким це необхідно для виконання їх робочих обов'язків, обмежуючи привілеї до мінімального рівня необхідного доступу.

2. Принцип необхідного доступу: Користувачі повинні мати доступ лише до тих ресурсів та інформації, які необхідні для виконання їх робочих функцій.

3. Принцип безпеки за замовчуванням: Системи та мережі повинні мати вбудовані заходи безпеки в режимі за замовчуванням, щоб забезпечити максимальний рівень захисту.

4. Принцип розділення обов'язків: Розділити обов'язки та доступ до ресурсів між різними користувачами або групами користувачів, щоб уникнути конфліктів інтересів та мінімізувати можливість зловживання.

5. Принцип захисту інформації від початку до кінця: Забезпечення захисту інформації від її створення до знищення, включаючи захист під час передачі, зберігання та обробки.

6. Принцип непередбачуваності та недоступності зловмисникам: Застосування заходів, що роблять атаку непередбачуваною та ускладненою для зловмисників, таких як шифрування, аутентифікація та моніторинг.

Ці принципи визначають основу для побудови ефективних стратегій і систем захисту в інформаційній сфері.

**2. Кіберзагрози та кібератаки**

**2.1 Поняття загроз, атак, вразливості.**

Загроза - це потенційна небезпека або шкода, яку можуть заподіяти шкідливі програми або зловмисні дії. Атака - це конкретний інцидент або дія, спрямована на вразливість для завдання шкоди або отримання доступу до системи чи даних.

Вразливість - це слабке місце в системі, яке може бути використане для проведення атаки або викликати непередбачені проблеми з безпекою.

**2.2 Класифікація загроз, атак.**

Класифікація загроз і атак у сфері кібербезпеки допомагає розуміти різноманітність шкідливих дій і ризиків, що стикаються з інформаційною безпекою. Ось деякі основні типи класифікації:

1. За джерелом атаки:

- Внутрішні атаки: Здійснюються зсередини організації, часто співробітниками або особами з доступом до систем.

- Зовнішні атаки: Походять ззовні і можуть бути проведені з метою нанесення шкоди системі або отримання конфіденційної інформації.

2. За типом атаки:

- Фішинг: Використовує соціальну інженерію для отримання конфіденційної інформації, такої як паролі чи особисті дані.

- Віруси та програми-шпигуни: Шкідливі програми, що поширюються через інтернет або електронну пошту та призначені для нанесення шкоди або збору інформації.

- DDoS-атаки: Атаки, спрямовані на перевантаження серверів або мережі шляхом надмірного навантаження запитами.

- Ман-в-середині (Man-in-the-Middle): Атаки, де зловмисник вступає між комунікаційними сторонами з метою перехоплення інформації або модифікації передачі даних.

3. За метою атаки:

- Спроможність до витоку даних: Атаки, спрямовані на отримання конфіденційної інформації, такої як фінансові дані або персональні дані користувачів.

- Нанесення шкоди системі: Атаки, які мають на меті нанести шкоду функціонуванню системи, видалити або пошкодити дані.

**2.3 Кіберзлочини. Кібервійна. Кібероборона.**

Кіберзлочини - це злочинні дії, які виконуються через інтернет або інші комп'ютерні мережі. Це може включати такі дії, як крадіжка конфіденційної інформації, шахрайство, атаки на комп'ютерні системи та інше.

Кібервійна - це форма конфлікту, в якій держави або групи ведуть боротьбу через комп'ютерні мережі. Це може включати кібератаки на важливі інфраструктурні об'єкти, спроби заволодіти чутливою інформацією або дестабілізувати супротивника.

Кібероборона - це набір заходів, спрямованих на захист від кіберзлочинів і кібервійни. Це може включати розвиток захисних програмних засобів, моніторинг за загрозами в мережах, навчання персоналу з питань кібербезпеки та інші заходи, спрямовані на забезпечення безпеки інформаційних систем.

**2.4 Кібертероризм. Кіберрозвідка.**

Кібертероризм - це використання комп'ютерних технологій для здійснення терористичних актів або для сприяння терористичним організаціям. Це може включати атаки на критичну інфраструктуру, розповсюдження пропаганди через інтернет, кібершпигунство та інші дії з метою завдання шкоди або створення паніки серед населення.

Кіберрозвідка - це збір інформації з використанням комп'ютерних технологій. Це може включати здійснення кібершпигунства для отримання конфіденційної інформації про політичних опонентів, військові цілі, торгові та економічні секрети та інші конфіденційні дані. Кіберрозвідка може проводитися як державними органами, так і приватними або злочинними групами з різних мотивів.

**2.5 Модель порушника.**

Модель порушника - це концептуальна модель, яка описує типового зловмисника чи порушника безпеки в контексті кібербезпеки. Ця модель допомагає розуміти мотивації, цілі, методи та характеристики атак, що можуть виявитися від різних типів загроз.

Типова модель порушника включає такі аспекти:

1. Мотивація: Може бути фінансовою, політичною, ідеологічною або просто вандалізмом. Наприклад, зловмисники можуть бути зацікавлені у вибутті з прибутків, викраденні конфіденційної інформації, завданні шкоди чи отриманні влади.

2. Методи атак: Це може включати використання вразливостей програмного забезпечення, соціальної інженерії, фішингу, вибіркової атаки на слабкі місця в мережі або в системі безпеки.

3. Цілі атак: Це може бути отримання доступу до конфіденційної інформації, викрадення грошей, розповсюдження вірусів, створення хаосу чи виклик недовіри до системи.

4. Характеристики: Модель порушника може також враховувати його технічні знання, рівень доступу до ресурсів та інші фактори, які впливають на його здатність та можливості для проведення атак.

Розуміння моделі порушника допомагає розробити ефективні заходи захисту та реагування на потенційні загрози в сфері кібербезпеки.

**2.6 Поняття, сутність та основні завдання комплексної системи захисту інформації.**

Комплексна система захисту інформації - це набір технічних, організаційних і правових заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в організації або системі. Основні поняття, сутність та завдання такої системи включають:

1. Поняття: Це включає в себе розуміння різних аспектів безпеки інформації, таких як конфіденційність (збереження конфіденційної інформації), цілісність (захист від несанкціонованого доступу чи модифікацій) та доступність (забезпечення доступу до інформації для авторизованих користувачів).

2. Сутність: Комплексна система захисту інформації є системою заходів, які мають на меті захистити інформацію від різних загроз, включаючи кіберзлочини, кібератаки, недбале ставлення до безпеки та інші ризики.

3. Основні завдання:

- Ідентифікація загроз і ризиків: Аналізується потенційні загрози для визначення ризиків для інформаційної системи.

- Розробка заходів захисту: Розробляються технічні, організаційні та правові заходи для запобігання загрозам та мінімізації ризиків.

- Впровадження та вдосконалення: Заходи захисту інформації реалізуються в організації, а також постійно вдосконалюються відповідно до змінних умов та загроз.

- Моніторинг та виявлення інцидентів: Здійснюється постійний моніторинг і виявлення можливих інцидентів безпеки для негайної реакції.

- Реагування на інциденти: При потребі вживаються заходи для ліквідації виявлених загроз та відновлення нормального функціонування системи.

**3. Безпека мережі**

**3.1 Поняття про шкідливе програмне забезпечення.**

Шкідливе програмне забезпечення (англ. malware) - це програми, створені з метою завдання шкоди комп'ютерам, мережам або користувачам. Вони можуть виконувати різноманітні дії, такі як видалення, крадіжка чи розповсюдження конфіденційної інформації, пошкодження файлів, перешкоджання нормальному функціонуванню ПК, атаки на інші комп'ютери тощо. Шкідливе програмне забезпечення може включати в себе віруси, черв'яки, троянські коні, шпигунське програмне забезпечення та інші види загроз.

**3.2 Шпигунські програми, фішинг, програми-вимагачі.**

Звичайні способи атаки включають шпигунське програмне забезпечення, яке намагається збирати конфіденційну інформацію без дозволу користувача; фішинг, що полягає в обмані користувачів з метою отримання їхніх особистих даних; і програми-вимагачі, які блокують доступ до файлів або системи користувача з метою вимагання викупу. Ці види загроз можуть завдати серйозної шкоди як комп'ютерам, так і користувачам.

**3.3 DdoS-атаки.**

DDoS-атаки (розподілені заперечення обслуговування) - це атаки, призначені для перевантаження системи чи мережі, заборони доступу до них для легітимних користувачів. У таких атаках зловмисники використовують багато комп'ютерів або пристроїв, що називається ботнетом, для одночасного надсилання великої кількості запитів до цільового сервера чи мережі. Це призводить до перевантаження ресурсів та відмови у обслуговуванні для легітимних користувачів, що може спричинити великі збитки для компаній чи організацій. Такі атаки часто мають на меті вимагати викуп за припинення атаки або просто завдати шкоди репутації чи фінансовим інтересам цільової організації.