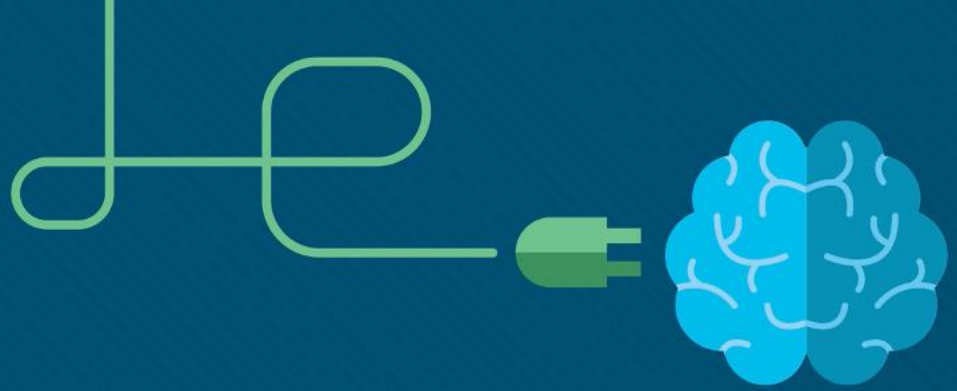


Розділ 1. Вступ до Кібербезпеки

Вступ до кібербезпеки (I2CS)

Мета розділу

Розділ 1. Вступ до кібербезпеки

Мета розділу: Пояснити основи безпеки в Інтернеті, зокрема, що таке кібербезпека та її потенційний вплив.

Назва теми	Мета вивчення теми
Світ кібербезпеки	Пояснити основи безпеки в Інтернеті, зокрема, що таке кібербезпека та її потенційний вплив.
Корпоративні дані	Визначити типи конфіденційної інформації, яку хакери можуть використати, щоб вторгнутися у ваше приватне життя та/або завдати шкоди вашій репутації, де вони можуть отримати доступ до цієї інформації та чому вона становить інтерес для кіберзлочинців.
Що було зроблено?	Пояснити, що таке корпоративні дані та чому їх важливо захищати.
Кібер-зловмисники	Описати, хто такі кіберзловмисники та чого вони хочуть.
Кібервійни	Пояснити, що таке кібервійна і чому країни та уряди потребують фахівців з кібербезпеки, щоб захистити своїх громадян та інфраструктуру.

1.1 Світ кібербезпеки

Що таке кібербезпека?

- Кібербезпека — це постійні зусилля щодо захисту окремих осіб, організацій та держави від цифрових атак шляхом захисту мережних систем і даних від несанкціонованого використання або пошкодження.

- **Особистий рівень:** На особистому рівні вам потрібно захистити вашу ідентичність, ваші дані та ваші електронні пристрої.

- **Корпоративний рівень:** На корпоративному рівні відповідальність кожного співробітника полягає в захисті репутації організації, її даних та клієнтів.

- **Державний рівень:** Оскільки все більше цифрової інформації збирається та розповсюджується, її захист стає ще важливішим на державному рівні, де на карті стоїть національна безпека, економічна стабільність, безпека та добробут громадян.

Захист ваших персональних даних

- Персональні дані – це будь-яка інформація, яка може бути використана для вашої ідентифікації, і вона може існувати як офлайн, так і онлайн.

- **Офлайн ідентичність**
  - Це реальна особистість, яку ви щодня представляєте вдома, у школі чи на роботі.
  - В результаті сім'я та друзі знають деталі вашого особистого життя, зокрема повне ім'я, вік та адресу.
  - Важливо не забувати про важливість захисту вашої особи в реальному житті.
  - Крадії особистих даних можуть легко вкрасти ваші дані прямо під носом, коли ви не бачите!

- **Онлайн ідентичність**
  - Це те, хто ви і як ви представляєте себе іншим особам в Інтернеті.
  - Вона містить ім'я користувача або псевдонім, який ви використовуєте для своїх онлайн-облікових записів, а також соціальну ідентичність, яку ви створюєте та показуєте в онлайн-спільнотах і на веб-сайтах.
  - Вам слід подбати про обмеження кількості персональної інформації, яку ви розкриваєте через свою особистість в Інтернеті.

Ваші дані

- Особисті дані описують будь-яку інформацію про вас, зокрема ваше ім’я, номер соціального страхування, номер водійських прав, дату і місце народження, дівоче прізвище вашої матері і навіть фотографії чи повідомлення, якими ви обмінюєтеся з родиною та друзями.
- Кіберзлочинці можуть використовувати цю конфіденційну інформацію, щоб ідентифікувати вас і видати себе за вас, порушуючи вашу конфіденційність і потенційно завдаючи серйозної шкоди вашій репутації.

Хакери можуть заволодіти вашими особистими даними через такі записи:

Медичні записи	Щоразу, коли ви відвідуєте лікаря, особиста інформація про ваше фізичне та і психічне здоров’я та благополуччя додається до ваших електронних медичних записів (EHR). Оскільки більшість цих записів зберігаються в Інтернеті, ви повинні знати про медичну інформацію, якою ви ділитеся. І ці записи виходять за межі кабінету лікаря.
Дані про освіту	Документи про освіту містять інформацію про вашу академічну кваліфікацію та досягнення. Крім того, записи можуть містити контактну інформацію, записи про стан здоров'я та вакцинації, а також записи про спеціальну освіту, включно з індивідуальними освітніми програмами (IEP).
Записи про працевлаштування та фінансова документація	Дані про зайнятість можуть бути цінними для хакерів, якщо вони можуть зібрати інформацію про вашу минулу роботу або навіть ваші поточні оцінки ефективності.Ваші фінансові записи можуть містити інформацію про ваші доходи та витрати. Ваші податкові записи можуть включати чеки заробітної плати, виписки з кредитної картки, ваш кредитний рейтинг та дані вашого банківського рахунку.

Де знаходяться ваші дані?

Лише вчора ви поділилися парою фотографій свого першого робочого дня з кількома своїми близькими друзями.Але це має бути нормально, правда? Подивимось…

- Ви зробили кілька фотографій на роботі на мобільний телефон.
- Копії цих фотографій тепер доступні на вашому мобільному пристрої.
- Ви поділилися цим з п’ятьма близькими друзями, які живуть у різних місцях по всьому світу.
- Усі ваші друзі завантажили фотографії і тепер мають копії ваших фотографій на своїх пристроях.
- Один із ваших друзів так пишався, що вирішив опублікувати ваші фотографії та поділитися ними в Інтернеті.
- Фотографії тепер не тільки на вашому пристрої.
- Насправді вони опинилися на серверах, розташованих у різних частинах світу, і люди, яких ви зараз навіть не знаєте, мають доступ до ваших фотографій.

1.1.6 Що ще?

- Це лише один приклад, який нагадує нам, що кожного разу, коли ми збираємо або передаємо персональні дані, ми повинні думати про нашу безпеку.
- В кожній країні діють свої закони, які захищають вашу конфіденційність та дані.
- Але чи знаєте ви, де саме знаходяться ваші дані?
  - Після призначення лікар оновить вашу медичну карту.
    - Для покриття страхових витрат ці відомості можуть надсилатись до страхової компанії.
    - У таких випадках ваша медична карта або її частина тепер доступні в страховій компанії.
  - Картки постійних покупців магазинів можуть бути зручним способом заощадити кошти на покупках.
    - Однак магазин використовує цю картку для створення профілю вашої купівельної поведінки, який потім може використовувати, щоб націлити на вас спеціальні пропозиції від своїх маркетингових партнерів.

Розумні пристрої

- Поміркуйте, як часто ви використовуєте свої комп’ютерні пристрої для доступу до своїх особистих даних.
- Якщо ви вирішили не отримувати паперові виписки, ви, ймовірно, отримуєте доступ до цифрових копій виписок з банківського рахунку через веб-сайт вашого банку.
- А під час оплати рахунка велика ймовірність того, що ви переказали необхідні кошти через застосунок для мобільного банкінгу.
- Крім того, що комп'ютерні пристрої дають змогу отримувати доступ до вашої інформації, вони також можуть генерувати інформацію про вас.
- Переносні технології, такі як розумні годинники та трекери активності, збирають ваші дані для клінічних досліджень, моніторингу здоров’я пацієнтів, а також відстеження фізичної форми та самопочуття.
- Зі зростанням світового ринку фітнес-трекерів зростає ризик для ваших особистих даних.

Крадіжка ідентичності

- Не задовольняючись крадіжкою ваших грошей для короткострокової фінансової вигоди, кіберзлочинці інвестують у довгострокову вигоду від крадіжки особистих даних.

Медична крадіжка

- Зростання медичних витрат призвело до зростання крадіжок медичних даних, коли кіберзлочинці крадуть медичну страховку, щоб скористатися її перевагами для себе.
- Якщо це станеться, будь-які медичні процедури, проведені на ваше ім'я, будуть збережені у вашій медичній документації.

Банкінг

- Викрадення особистих даних може допомогти кіберзлочинцям отримати доступ до банківських рахунків, кредитних карток, соціальних профілів та інших облікових записів онлайн-сервісів.
- Зловмисник, який викрав ідентифікаційні дані, може подати підроблену податкову декларацію та одержати відшкодування.
- Вони навіть можуть брати позики на ваше ім'я і зруйнувати ваш кредитний рейтинг (і ваше життя також).

Кому ще потрібні мої дані?

- Ваші персональні дані шукають не лише злочинці.

- У таблиці описані інші суб'єкти, зацікавлені у вашій онлайн-ідентичності, і чому.

Ваш Інтернет-провайдер (ISP)	Ваш провайдер відстежує вашу онлайн-активність, і в деяких країнах вони можуть продавати ці дані рекламодавцям з метою отримання прибутку. За певних обставин провайдери Інтернету можуть бути за законом зобов'язані надавати вашу інформацію державним наглядовим органам або органам влади.
Рекламодавці	Таргетована реклама є частиною Інтернету. Рекламодавці відстежують вашу діяльність в Інтернеті, як-от купівельні звички та особисті уподобання, а також надсилають вам цільову рекламу.
Пошукові системи та платформи соціальних мереж	Ці платформи збирають інформацію про вашу стать, геолокацію, номер телефону, та політичну та релігійну ідеологію на основі вашої історії пошуку та онлайн-ідентичності. Потім ця інформація продається рекламодавцям для отримання прибутку.
Веб-сайти, які ви відвідуєте	Веб-сайти використовують файли cookie для відстеження вашої діяльності, щоб забезпечити більш персоналізований досвід. Але це залишає слід даних, пов'язаний з вашою ідентичністю в Інтернеті, який часто може опинитися в руках рекламодавців!

1.2 Корпоративні дані

Типи корпоративних даних

Традиційні дані зазвичай генеруються та обробляються всіма організаціями, великими та малими.

- Вони містять наступне:
  - **Дані про транзакції,** як-от деталі, що стосуються купівлі та продажу, виробничої діяльності та основних корпоративних операцій, наприклад будь-яка інформація, яка використовується для прийняття рішень щодо працевлаштування.
  - **Інтелектуальна власність,** така як патенти, торгові марки та плани випуску нових продуктів, дозволяє підприємству отримувати економічні переваги над своїми конкурентами. Ця інформація часто вважається комерційною таємницею, і її втрата може виявитися катастрофічною для майбутнього компанії.
  - **Фінансові дані,** такі як звіти про доходи, балансові звіти та інформація про рух грошових коштів, дають уявлення про фінансовий стан компанії.

1.2.1 Типи корпоративних даних (прод.)

Інтернет речей та великі дані

- **IoT** – це велика мережа фізичних об’єктів, таких як датчики, програмне забезпечення та інше обладнання.
- Усі ці «речі» підключені до Інтернету з можливістю збирати дані та обмінюватися ними.
- Можливості зберігання даних розширюються завдяки хмарі та віртуалізації.
- Це експоненціальне зростання даних створило нову область інтересу до технологій та бізнесу під назвою «Великі дані».

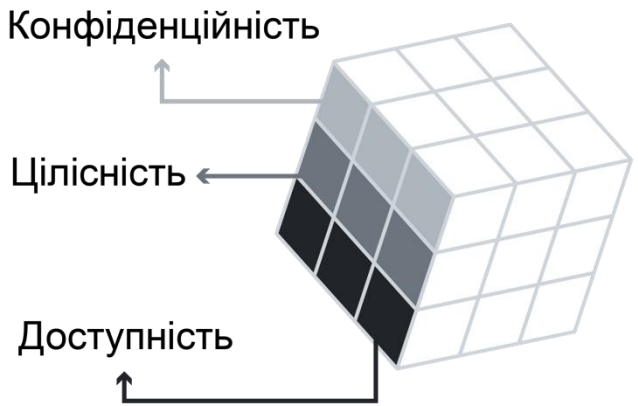
Куб

Ця модель безпеки має три виміри:

1. **Основоположні принципи захисту інформаційних систем.**

- **Конфіденційність** – це набір правил, що запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Методи забезпечення безпеки містять **шифрування даних**, **підтвердження особи** та **двофакторну автентифікацію**.
- **Цілісність** забезпечує захист системної інформації або процесів від навмисних або випадкових змін. Одним із способів забезпечити цілісність є використання **хеш-функції** або **контрольної суми**.
- **Доступність** означає, що авторизовані користувачі можуть отримати доступ до систем і даних, коли і де це необхідно, а ті, які не відповідають встановленим умовам, ні . Це може бути досягнуто за рахунок **обслуговування обладнання**, **проведення ремонту апаратного забезпечення**, **оновлення операційних систем та програмного забезпечення**, **і створення резервних копій**.

Основні принципи захисту інформації



Куб (прод.)

2. Захист інформації в кожному з її можливих станів

- **Обробка** відноситься до стану даних, що використовуються для виконання такої операції, як оновлення запису бази даних (дані в обробці).
- **Зберігання** визначає стан даних, що зберігаються в пам'яті або на пристрої постійного зберігання, такому як жорсткий диск, твердотілий накопичувач або USB-накопичувач (дані в стані спокою).
- **Передавання** відноситься до стану переміщення даних між інформаційними системами (дані в русі).

Куб (прод.)

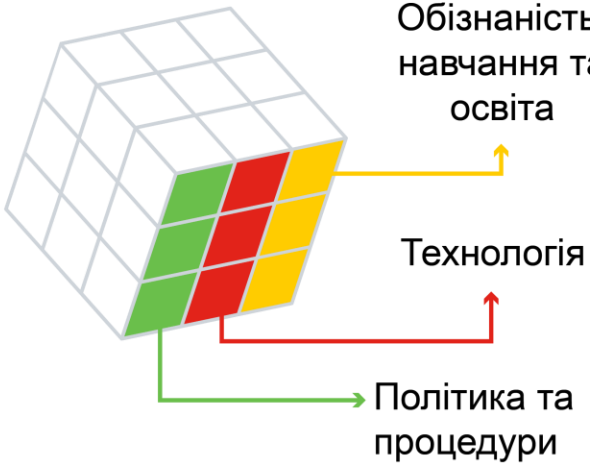
3. Заходи безпеки, які використовуються для захисту даних.

- **Обізнаність, навчання та освіта** – це заходи, які вживаються організацією, щоб гарантувати, що користувачі знають про потенційні загрози безпеці та дії, які вони можуть вжити для захисту інформаційних систем.

- **Технологія** відноситься до програмно-апаратних рішень, розроблених для захисту інформаційних систем, таких як брандмауери, які постійно контролюють вашу мережу в пошуках можливих шкідливих інцидентів.

- **Політика та процедури** відносяться до адміністративних засобів контролю, які забезпечують основу того, як організація реалізує інформаційну безпеку, наприклад плани реагування на інциденти та рекомендації з найкращих практик.

Заходи безпеки, що застосовуються для захисту даних



1.2.4 Чи це насправді?

- Так, фішинг дуже поширений і часто працює.
- Наприклад, у серпні 2020 року елітний ігровий бренд Razer зазнав злому даних, який розкрив особисту інформацію приблизно 100 000 клієнтів.
- Консультант з безпеки виявив, що хмарний кластер (група пов'язаних серверів, що забезпечують зберігання даних, бази даних, мережу та програмне забезпечення через Інтернет) був неправильно налаштований відкривши сегмент інфраструктури Razer для загальнодоступного Інтернету, що призвело до витоку даних.
- Razer знадобилося більше трьох тижнів, щоб захистити хмарний екземпляр від загального доступу, і протягом цього часу кіберзлочинці мали доступ до інформації про клієнтів, яка могла бути використана в соціальній інженерії та шахрайських атаках, як-от в тій атаці, яку ви щойно розкрили.
- Тому організаціям необхідно застосовувати проактивний підхід до хмарної безпеки, щоб забезпечити захист конфіденційних даних.

Порушення безпеки даних

- Наслідки порушення безпеки даних серйозні, але вони стають надто поширеними.
- Інтернет речей під'єднує все більше пристроїв, створюючи більше можливостей у кіберзлочинців для атаки.
- Два добре відомих порушення безпеки даних містять:

  - **Ботнет Persirai**
    - У 2017 році ботнет Інтернету речей (IoT) Persirai націлювався на понад 1000 різних моделей IP-камер, звертаючись до відкритих портів, щоб ввести команду, яка змушувала камери підключатися до сайту, який встановлював на них зловмисне програмне забезпечення.
    - Після того, як зловмисне програмне забезпечення було завантажено та запущене, воно видалялося, і тому могло працювати в пам’яті, щоб уникнути виявлення.
    - Понад 122 000 цих камер від кількох різних виробників були захоплені та використані для здійснення розподілених атак типу «Відмова в обслуговуванні» (DDoS) без відома їх власників.
    - DDoS-атака відбувається, коли кілька пристроїв, заражених шкідливим програмним забезпеченням, перевантажують ресурси цільової системи.

Порушення безпеки даних (прод.)

- **Equifax Inc.**
  - У вересні 2017 року Equifax, агентство споживчих кредитів у Сполучених Штатах, публічно оголосило про випадок витоку даних: зловмисники змогли використати вразливість у своєму програмному забезпеченні веб-застосунків, щоб отримати доступ до конфіденційних особистих даних мільйонів клієнтів.
  - У відповідь на це порушення Equifax створила спеціальний веб-сайт, який дозволив клієнтам Equifax визначити, чи була їхня інформація зламана.
  - Однак замість використання субдомену equifax.com компанія створила нове доменне ім’я, що дозволило кіберзлочинцям створювати неавторизовані веб-сайти з подібними іменами.
  - Ці веб-сайти використовувалися, щоб спробувати обдурити клієнтів надати особисту інформацію.
  - Зловмисники можуть використати цю інформацію, щоб визначити особу клієнта.
  - У таких випадках клієнту було б дуже важко довести протилежне, враховуючи, що хакер також володіє його особистими даними.

Наслідки порушення безпеки

Ці приклади показують, що потенційні наслідки порушення безпеки можуть бути серйозними.

Репутаційна шкода	Порушення безпеки може мати негативний довгостроковий вплив на репутацію організації, на створення якої знадобилися роки. Клієнтів, особливо тих, хто постраждав від порушення, необхідно буде повідомити, і вони можуть вимагати компенсації та/або звернутися до надійного та безпечного конкурента. Співробітники також можуть вирішити звільнитися у світлі скандалу. Залежно від серйозності порушення, відновлення репутації організації може зайняти багато часу.
Вандалізм	Хакер або хакерська група може зруйнувати веб-сайт організації, розміщуючи неправдиву інформацію. Вони можуть навіть внести кілька незначних змін у номер телефону або адресу вашої організації, що може бути складніше виявити.У будь-якому випадку онлайн-вандалізм може вказувати на ваш непрофесіоналізм і негативно вплинути на репутацію та авторитет вашої організації.
Крадіжка	Порушення захисту часто пов’язане з інцидентом, коли конфіденційні персональні дані були вкрадені. Кіберзлочинці можуть оприлюднити цю інформацію або використати її для крадіжки грошей та/або ідентичності.
Втрати доходу	Фінансові наслідки порушення безпеки можуть бути руйнівними. Наприклад, хакери можуть зламати веб-сайт організації, не даючи їй вести бізнес в Інтернеті. Втрата інформації про клієнта може перешкодити зростанню та розширенню компанії. Це може вимагати подальших інвестицій в інфраструктуру безпеки організації. І не забуваймо, що організаціям можуть загрожувати великі штрафи, якщо вони не захищають дані в Інтернеті.
Порушення прав інтелектуальної власності	Порушення безпеки також може мати руйнівний вплив на конкурентоспроможність організації, особливо якщо хакери зможуть отримати у свої руки конфіденційні документи, комерційну таємницю та інтелектуальну власність.

1.3 Що було викрадено?

Сценарій 1

- Порушення безпеки сьогодні є дуже поширеними, зловмисники постійно знаходять нові та інноваційні способи проникнення в організації в пошуках цінної інформації.
- Розглянемо наступні два вигадані сценарії.

Сценарій 1:

- Згідно з нашими джерелами, відома мережа готелів, що функціонує в усьому світі, повідомила про масовий злом даних, особисту інформацію понад трьох мільйонів гостей отримали хакери.

- Готель виявив, що хакери отримали доступ до його бази даних клієнтів, використовуючи дані для входу одного з його співробітників.

- На даний момент в готелі не вірять, що хакери змогли отримати доступ до паролів облікових записів або фінансової інформації.

- Недавнім гостям пропонується перевірити веб-портал мережі готелів, щоб дізнатися, чи не постраждали вони від цього порушення.

Сценарій 2

Сценарій 2:

- Команда @Apollo стурбована. Платформи електронного навчання стають головними цілями для зловмисників, оскільки все більше організацій переходять на цифрове навчання.
- Популярна онлайн-платформа для навчання визнала, що особисті дані мільйонів її студентів (багато з них неповнолітніх) розкрито у загальнодоступній хмарній базі даних.
- Хакери змогли отримати прямий доступ до повних імен учнів, адрес електронної пошти, номерів телефонів та інформації про зарахування до школи з Інтернету!
- Хоча незрозуміло, що хакери зробили з цією отриманою інформацією, можна з упевненістю сказати, що у них є все необхідне для здійснення широкомасштабних фішингових або шкідливих атак.

Ключові моменти

- Порушення безпеки – це інцидент, який призводить до несанкціонованого доступу до даних, програм, служб або пристроїв, розкриваючи особисту інформацію, яку зловмисники можуть використовувати для отримання фінансової вигоди або інших переваг.
- Але є багато способів захистити себе та свою організацію.
- Важливо знати про поширені кіберзагрози та залишатися пильними, щоб не стати наступною жертвою.

Дізнатися більше

Знайдіть кілька додаткових прикладів нещодавніх порушень безпеки.

- У кожному конкретному випадку ви можете визначити:
  - що викрадено?
  - які експлойти використали зловмисники?
  - які дії можна вжити, щоб запобігти повторенню порушення в майбутньому?

1.4Кібер-зловмисники

Класифікація зловмисників

- Кібер-зловмисники варіюються від аматорів до добре організованих і намагатимуться будь-що, щоб отримати особисту інформацію.
- Їх часто відносять до категорії нападників у білих капелюхах, у сірих капелюхах або у чорних капелюхах .

Хакери-аматори

- Термін «script kiddies» з'явився в 1990-х роках і стосується недосвідчених хакерів-любителів, які використовують наявні інструменти чи інструкції, знайдені в Інтернеті, для запуску атак.
- Деякі з них роблять це просто з цікавості, а інші намагаються продемонструвати свою майстерність і заподіяти шкоду.
- Хоча ці зловмисники можуть використовувати прості інструменти, їхні атаки все одно можуть мати руйнівні наслідки.

Типи зловмисників (прод.)

Хакери

- Це група зловмисників, яка зламує комп'ютери або мережі з метою отримання доступу.

- Залежно від наміру вторгнення ці зловмисники класифікуються як Білі, Сірі або Чорні капелюхи.
  - **Білі капелюхи** втручаються в мережі або комп'ютерні системи, щоб виявити слабкі місця та покращити безпеку цих систем.Такі вторгнення виконуються за попереднім дозволом і всі результати повідомляються власнику.

  - **Зловмисники в сірих капелюхах** можуть шукати вразливості в системі, але вони повідомлятимуть про свої висновки власникам системи, лише якщо це збігається з їх зацікавленістю. Вони можуть публікувати факти про вразливість в Інтернеті, щоб інші нападники могли нею скористатися.

  - **Чорні капелюхи** використовують будь-яку вразливість для отримання незаконної особистої, фінансової або політичної користі.

Класифікація зловмисників (прод.)

Організовані хакери

- До таких хакерів відносяться організації кіберзлочинців, хактивісти, терористи та хакери, що фінансуються державою.
- Ці злочинці висококваліфіковані та організовані і навіть можуть надавати кіберзлочин, як сервіс іншим злочинцям.
- Хактивісти роблять політичні заяви, щоб привернути увагу до важливих для них проблем.
- Хакери, спонсоровані державою, здійснюють розвідку або диверсії від імені своєї держави.
- Ці нападники зазвичай якісно підготовлені та добре фінансуються, а їх атаки зосереджені на корисних для їх держави конкретних цілях.

Внутрішні і зовнішні загрози

- Кібератаки можуть виникати як всередині організації, так і ззовні.

- **Внутрішні**
  - Співробітники, контрактний персонал або надійні партнери можуть випадково або навмисно:
    - неправильно поводитися з конфіденційними даними
    - сприяти зовнішнім атакам, підключивши заражений USB-носій до корпоративної комп'ютерної системи
    - заносити шкідливе програмне забезпечення до мережі організації, відкриваючи шкідливі електронні листи або веб-сайти
    - загрожувати роботі внутрішніх серверів або пристроїв мережної інфраструктури.

- **Зовнішні**
  - Любителі або кваліфіковані зловмисники за межами організації можуть:
    - використовувати вразливі місця в мережі
    - отримувати неавторизований доступ до комп'ютерних пристроїв
    - використовувати соціальну інженерію для отримання несанкціонованого доступу до корпоративних даних.

1.5 Кібервійни

Ознака часу (Stuxnet)

- Одним із прикладів атаки, спонсорованої державою, було зловмисне програмне забезпечення Stuxnet, яке було розроблено не просто для захоплення цільових комп'ютерів, а й для того, щоб фактично завдати фізичної шкоди обладнанню, яке контролюється комп'ютерами!

- Натисніть кнопку відтворення, щоб переглянути коротке відео про інцидент Stuxnet і дізнатися, який вплив це зловмисне програмне забезпечення справило на іранський завод зі збагачення урану.

Мета кібервійни

- Основна мета кібервійни - отримати перевагу над супротивниками, незалежно від того, чи є вони державами або конкурентами.
- Кібервійна використовується в наступних випадках:

- **Для збору скомпрометованої інформації та/або секретів захисту**

  - Нація або міжнародна організація можуть брати участь у кібервійні, щоб викрасти секрети захисту та зібрати інформацію про технології, які допоможуть скоротити відставання в індустрії та військових можливостях.

  - Крім того, скомпрометовані конфіденційні дані надають нападникам можливість шантажу членів уряду.

Мета кібервійни (прод.)

- **Вплинути на інфраструктуру іншої країни**
  - Окрім промислового та військового шпигунства, нація може постійно атакувати інфраструктуру іншої країни, щоб викликати крах і хаос.
  - Наприклад, атака може зруйнувати енергосистему великого міста.
  - Подумайте про наслідки, якщо це станеться; дороги будуть перевантажені, обмін товарами та послугами буде припинено, пацієнти не зможуть отримати необхідну допомогу у разі надзвичайних ситуацій, доступ до Інтернету буде перервано.
  - Через відключення електромережі кібератака може мати величезний вплив на повсякденне життя пересічних громадян.

1.6 Контрольна робота

Що нового я дізнався у цьому розділі?

- Кібербезпека — це постійні зусилля щодо захисту окремих осіб, організацій та держави від цифрових атак шляхом захисту мережних систем і даних від несанкціонованого використання або пошкодження.
- Персональні дані – це будь-яка інформація, яка може бути використана для вашої ідентифікації, і вона може існувати як офлайн, так і онлайн.
- Традиційні дані зазвичай генеруються та обслуговуються всіма організаціями, великими та малими.
- Куб МакКамбера — це модель, створена Джоном МакКамбером у 1991 році, щоб допомогти організаціям створити та оцінити ініціативи з інформаційної безпеки, враховуючи всі пов’язані фактори, які на них впливають.
- Порушення безпеки може мати негативний довгостроковий вплив на репутацію організації, на створення якої знадобилися роки.
- Порушення захисту часто пов’язане з інцидентом, коли конфіденційні персональні дані були вкрадені.
- Кіберзлочинці можуть оприлюднити цю інформацію або використати її для крадіжки грошей та/або ідентичності.
- Кібератаки можуть виникати як всередині організації, так і ззовні.