Самостійна робота 7
Особисті та корпоративні дані. Технології зберігання

Інформаційні ресурси
Курс «Кібербезпека» Міжнародної мережевої академії CISCO
https://legacy.netacad.com/portal/welcome-to-legacy-netacad.

Вивчити матеріал 1 розділу курсу «Кібербезпека» Міжнародної мережевої академії CISCO

Контрольні питання:
1. Дайте визначення даним. Які є типи даних?
2. Де можуть зберігатися дані?
3. Які існують технології зберігання даних з точки зору кібербезпеки?

Вид контролю

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.

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).

Типи корпоративних даних

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

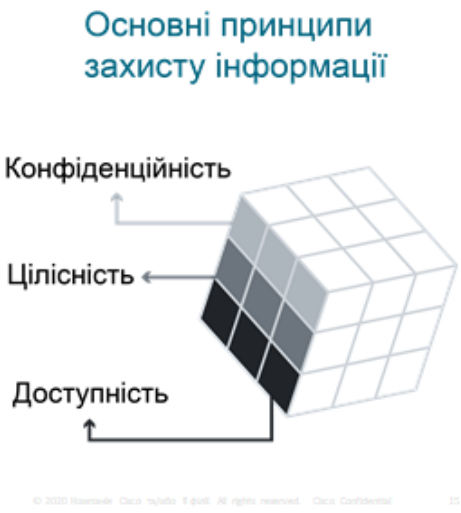
- Вони містять наступне:
  - **Дані про транзакції,** як-от деталі, що стосуються купівлі та продажу, виробничої діяльності та основних корпоративних операцій, наприклад будь-яка інформація, яка використовується для прийняття рішень щодо працевлаштування.
  - **Інтелектуальна власність,** така як патенти, 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.

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**.



1. Проаналізуйте інформацію.
2. Поясніть на прикладі кубу основних принципів захисту інформації як захистити особисті (І варіант) або корпоративні (ІІ варіант) дані.
3. Поясніть поняття «Інтернет речей IoT» та «Великі дані». До якого типу даних вони належать?

Обов’язково вказати джерела інформації