Лекція 2. Цифрова безпека бізнесу та кібер ризики підприємств в умовах цифрової економіки

Поняття цифрової безпеки

Цифрова безпека відноситься до різних способів захисту технічних пристроїв і файлів від вторгнення зовнішніми користувачами

включає інструменти, які використовуються для захисту:

- цифрової ідентичності
- активів
- технологій в сучасному цифровому світі

Правилами цифрової безпеки

- Необхідно використовувати ліцензійне програмне забезпечення у особистій і професійній діяльності (працюючи на різних пристроях)
- Оновлювати програмне забезпечення, встановлювати антивірусні програми та firewall (міжмережевий екран, фаєрвол)
- Встановлювати пароль на вхід у пристрій
- Використовувати менеджер паролів
- Не використовувати ненадійні поштові сервіси, соціальні мережі, месенджери

Правилами цифрової безпеки

- Необхідно розділяти облікові записи (поштові скриньки окремо для роботи і для дому)
- Блокувати пристрої на яких працює користувач
- Використовувати повнодискове шифрування пристроїв
- Видаляти історію з браузера та кеш
- Не зазначати очевидні відповіді для відновлення доступу до свого облікового запису

Правилами цифрової безпеки

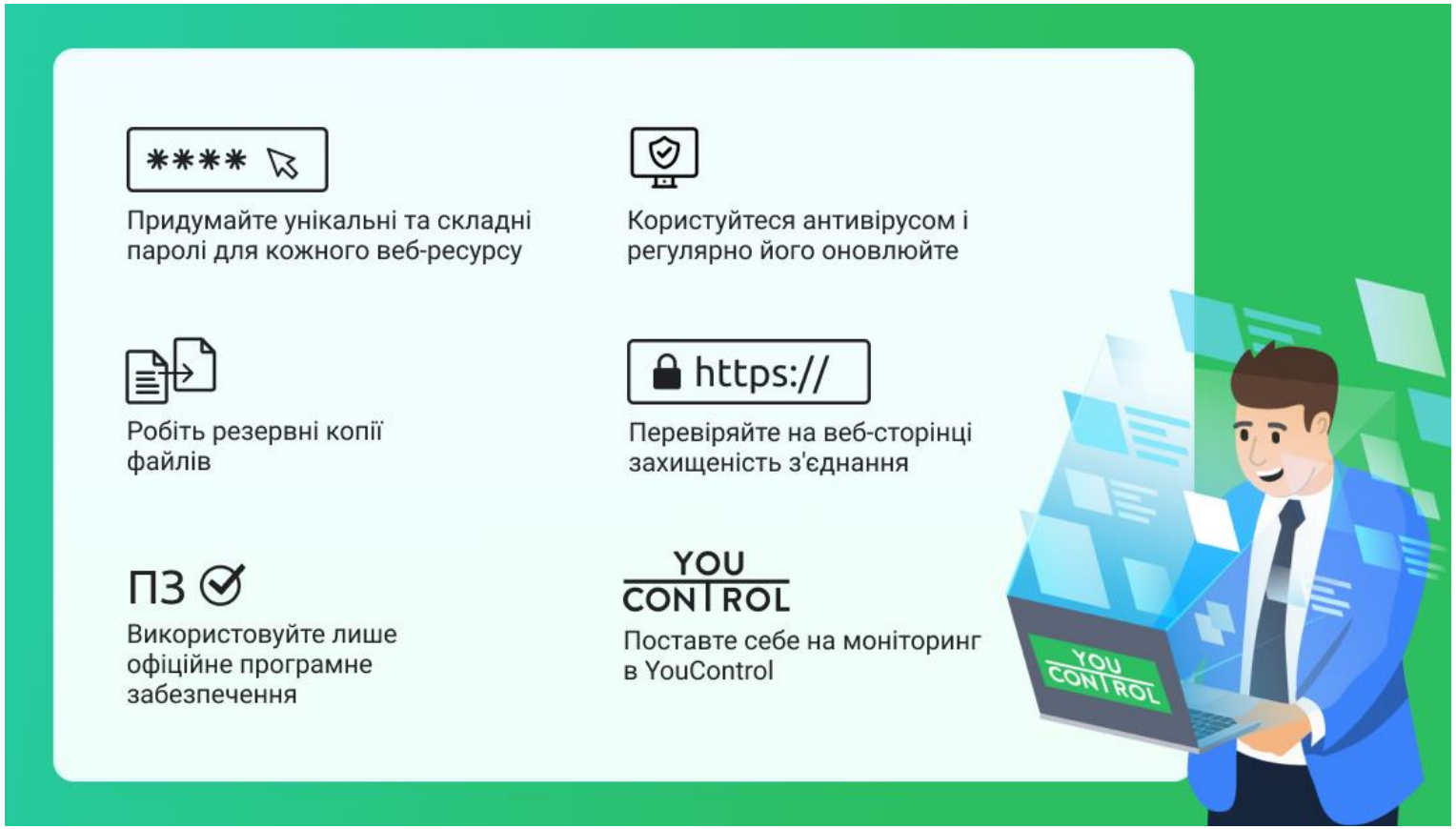
- Не використовувати для відновлення доступу незахищені поштові скриньки
- Користуватись секретними месенджерами, якщо вирішили вести таємну переписку
- Використовуйте месенджери з шифруванням від пристрою до пристрою
- Не переходити за підозрілими посиланнями
- Не ловитись на фішинг

Правилами цифрової безпеки

- Робити резервні копії важливих файлів в хмарних сховищах
- Робити двофакторну авторизацію для важливих облікових записів
- Використовувати технології VPN (Virtual Private Network - віртуальна приватна мережа) при підключенні до публічного wi-fi
- Використовувати мережу Tor, якщо користувач хоче бути анонімними
- Змінювати дефолтний пароль на домашньому wi-fi-роутері

Цифрова гігієна: основні характеристики

Цифрова гігієна в умовах кібератак та маніпуляцій: поради від YouControl



https://youcontrol.com.ua/en/

Найпоширеніші кібератаки

Кібератаки – це дії кіберзлочинців, спрямовані на комп'ютерні системи, бази даних, інфраструктуру і відвідувачів вебсайтів

Найпоширеніші **види кібератак**:

- фішин
- атаки програм-вимагачів
- шкідливе програмне забезпечення
- витік даних
- DDOS-атаки
- атака «ЛЮДИНА ПОСЕРЕДИНІ»
- SQL-ін'єкції
- міжсайтовий скріптинг (XXS)
- експлойт (експлуатація) нульового дня
- DNS-тунелювання
- атаки на паролі методом повного перебору, або брутфорс

Фішинг

Фішинг – це атака, яка в основному використовує електронну пошту як вектор та в обманний спосіб змушує людей завантажувати шкідливі програми на свої пристрої

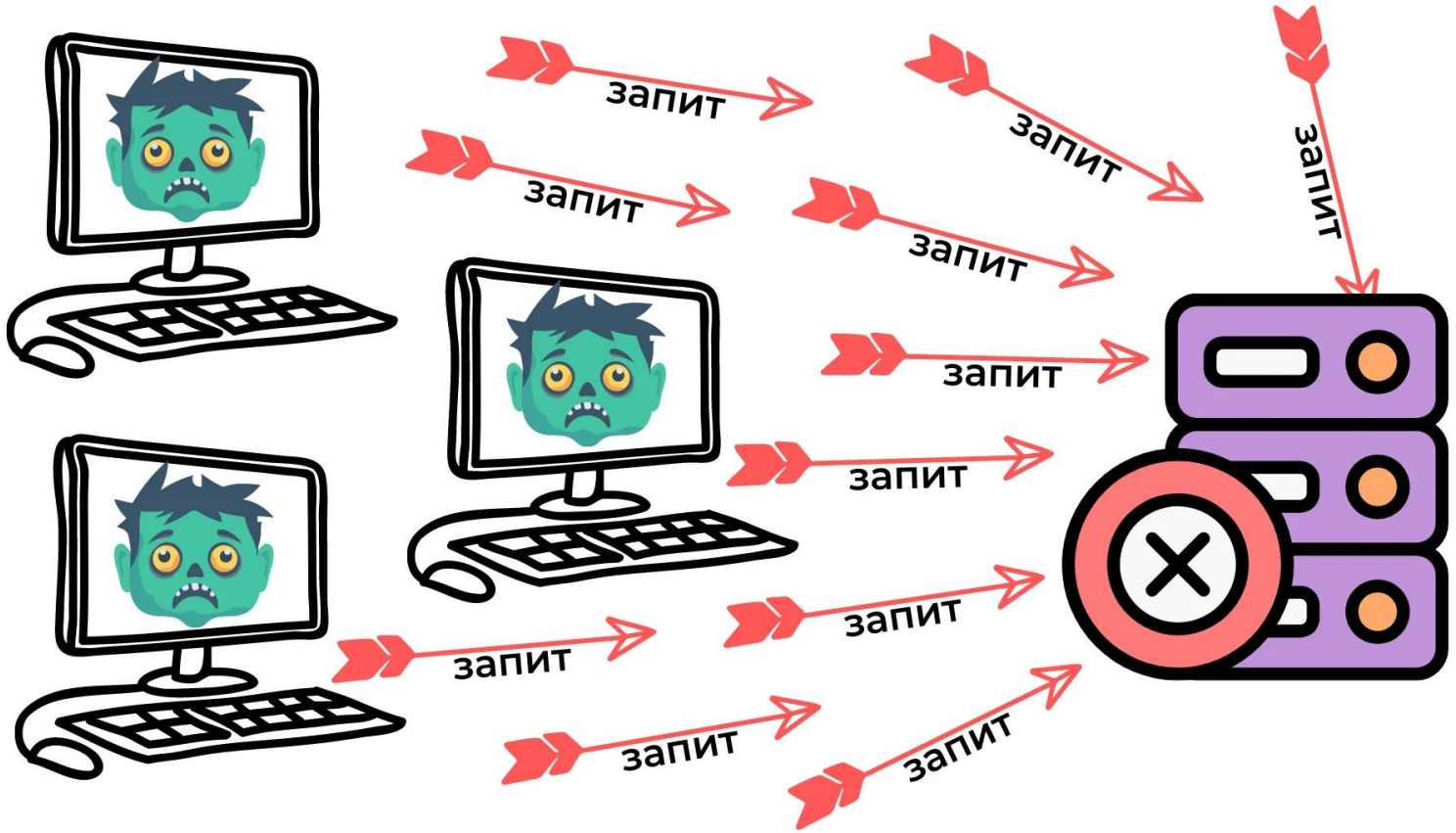
Види фішингу:

- **whaling** – атаки, спрямовані на керівників вищої ланки
- **smishing** – атаки, що використовують текстові або SMS-повідомлення, щоб привернути увагу жертви
- **vishing** – атака через голосову пошту
- **search engine phishing** – атаки, які за допомогою SEO підвищують у пошуковій видачі позиції сайтів потрібних злочинцям
- **email phishing** – атака через електронну пошту

Атаки програм-вимикачів, шкідливе ПЗ та витік даних

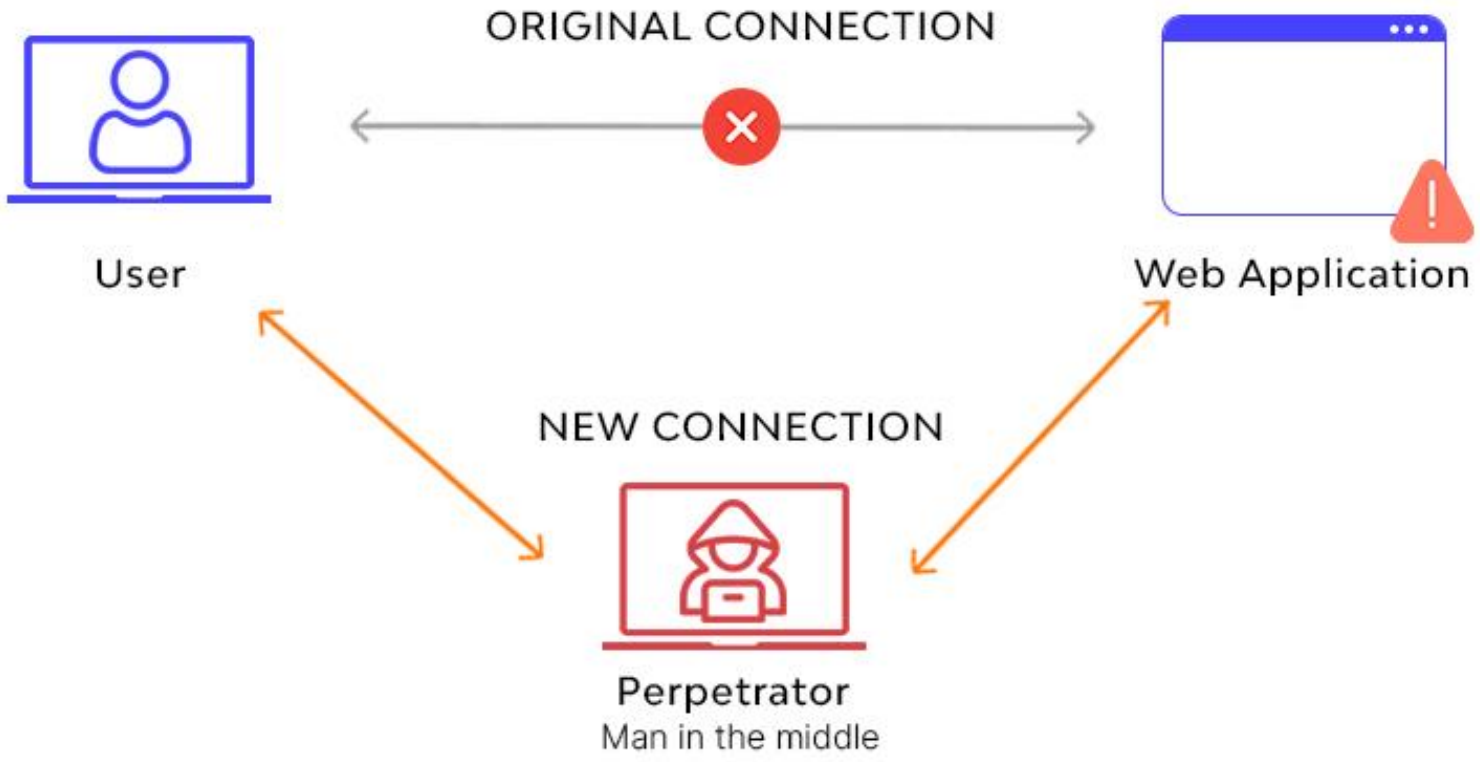
- **Програми-вимагачі (ransomware)** – це шкідливе ПЗ, яке блокує доступ користувачів до їхнього програмного забезпечення і вимагає заплатити викуп (ransomware поширюється за допомогою спаму або соціальної інженерії)
- **Шкідливі програми** зупиняють роботу пристроїв або значно уповільнюють їх. Програми-шпигуни, віруси, черв'яки, програми-вимагачі або програми-трояни – все це використовують кіберзлочинці
- **Витік даних** відбувається, коли конфіденційна інформація користувача стає вразливою

DDOS-атаки



- направляють великий обсяг трафіку до системи або сервера
- змушують зупинити або призупинити роботу

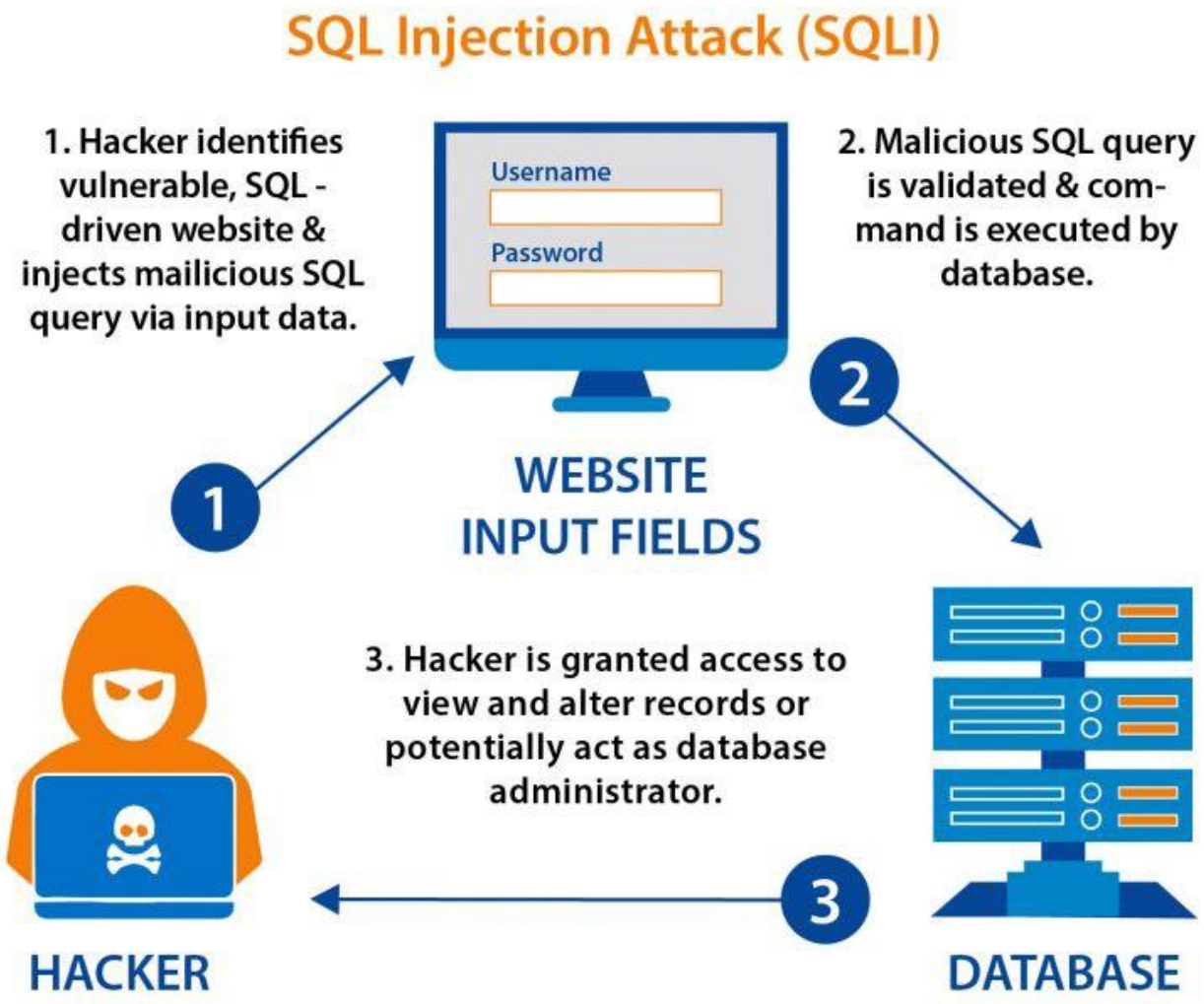
Атака «людина посередині» (MITM)



Типи атак «людина посередині»:

- Фальшиві точки доступу
- Address resolution spoofing
- mDNS spoofing
- DNS spoofing

SQL-ін'єкції

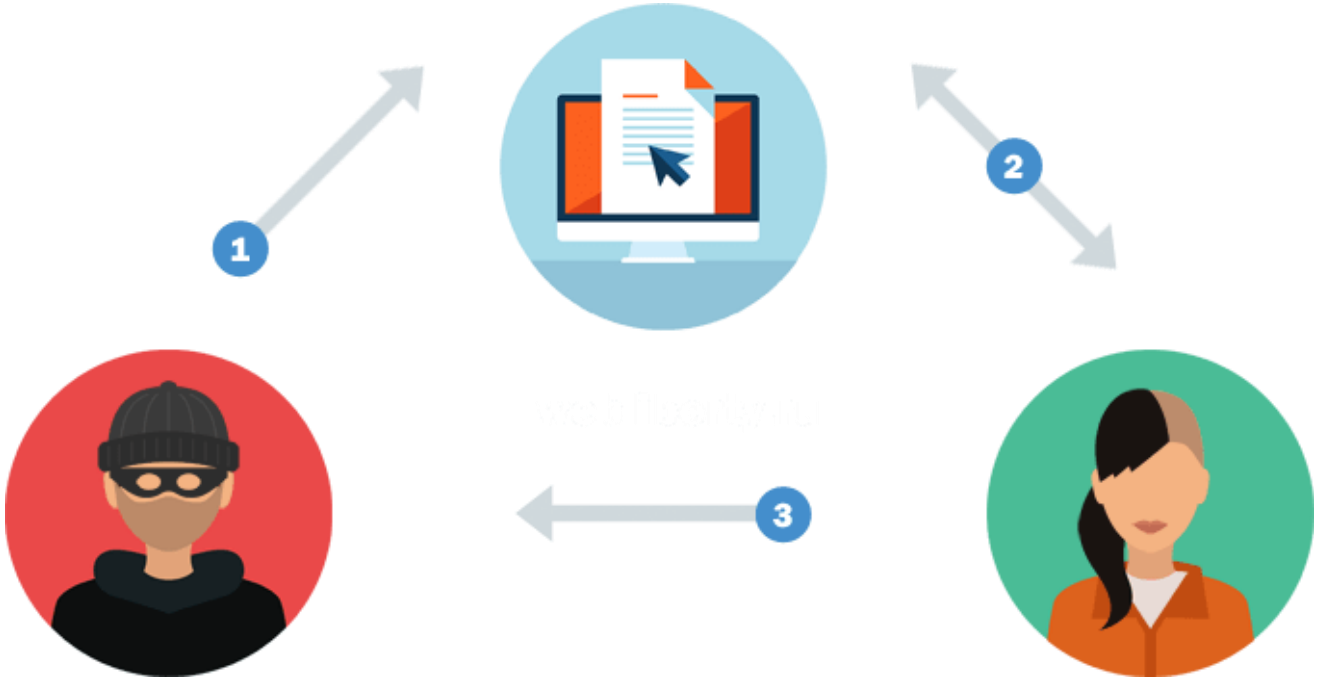


Атака може надати у розпорядження хакерів

- паролі та особисту інформацію
- змінити дані, які зберігаються в базі
- виконувати адміністративні операції
- відновлювати вміст файлів

Міжсайтовий скріптинг (XXS)

використовує шкідливий код для запуску певного сценарію у веббраузері або програмі



- замість безпосередньої атаки на сервер зловмисники використовують вразливий сервер для атаки на користувача
- код виконує шкідливий сценарій на комп’ютері жертви

Експлойт (експлуатація) нульового дня

зловмисник використовує вразливість Zero Day для атаки на систему

- групи кіберзлочинців використовують експлойти нульового дня стратегічно
- використовують їх в атаках на медичні чи фінансові установи, урядові організації

DNS-тунелювання

DNS-тунелювання

- атакаючий використовує DNS як маскування для обходу фаєрволу
- він тунелює протоколи поверх (наприклад HTTP, поверх DNS
- тунелює IP-трафік переміщує викрадені дані

- вкрадені дані реконструюються атакуючим
- даний тунель можна використовувати для завантаження шкідливого коду

Атаки на паролі методом повного перебору

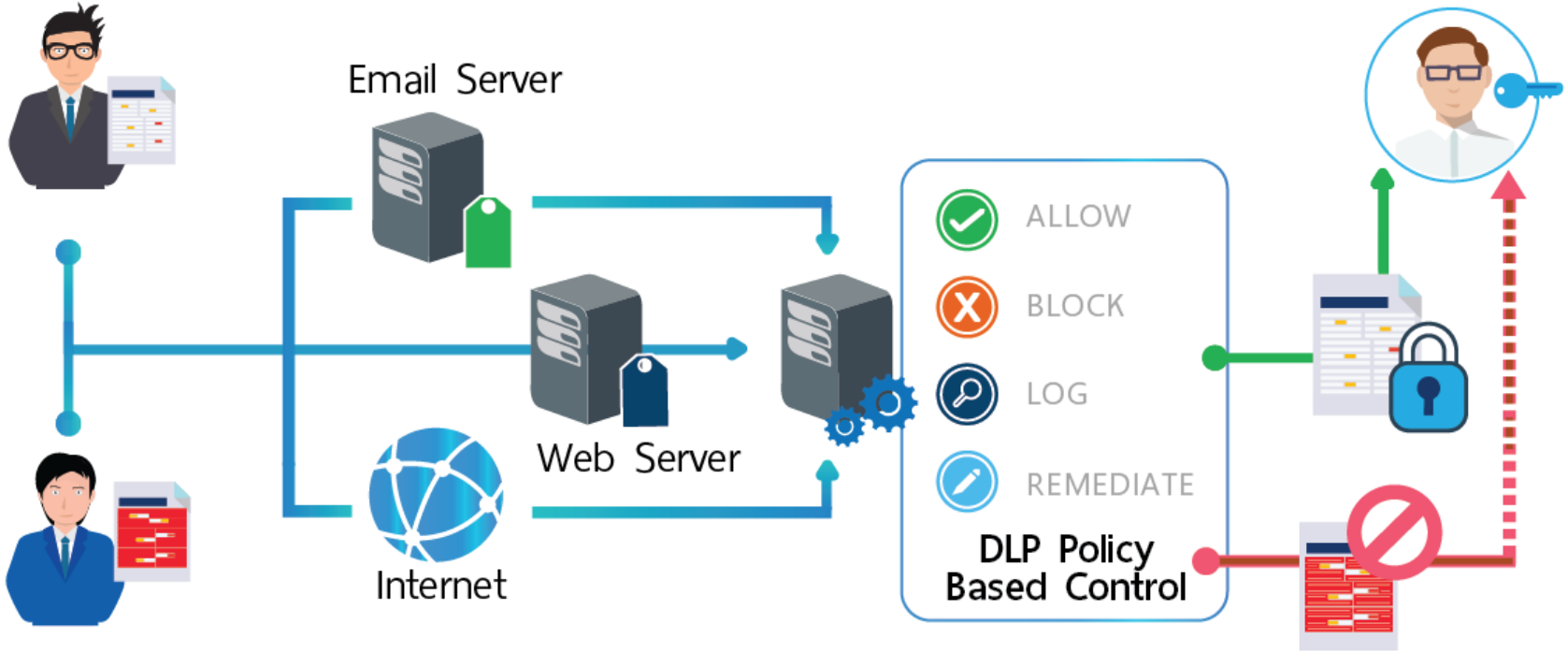
- способи захисту від брутфорсу
- не використовуйте «admin» в якості імені користувача
- використовуйте надійні паролі
- використовуйте на сайті двофакторну аутентифікацію
- обмежте спроби входу в адміністративну панель сайту
- використовуйте останні версії тем, плагінів і модулів

Ризики втрати корпоративної інформації

DLP - рішення для запобігання витоку конфіденційних файлів за межі мережі компанії

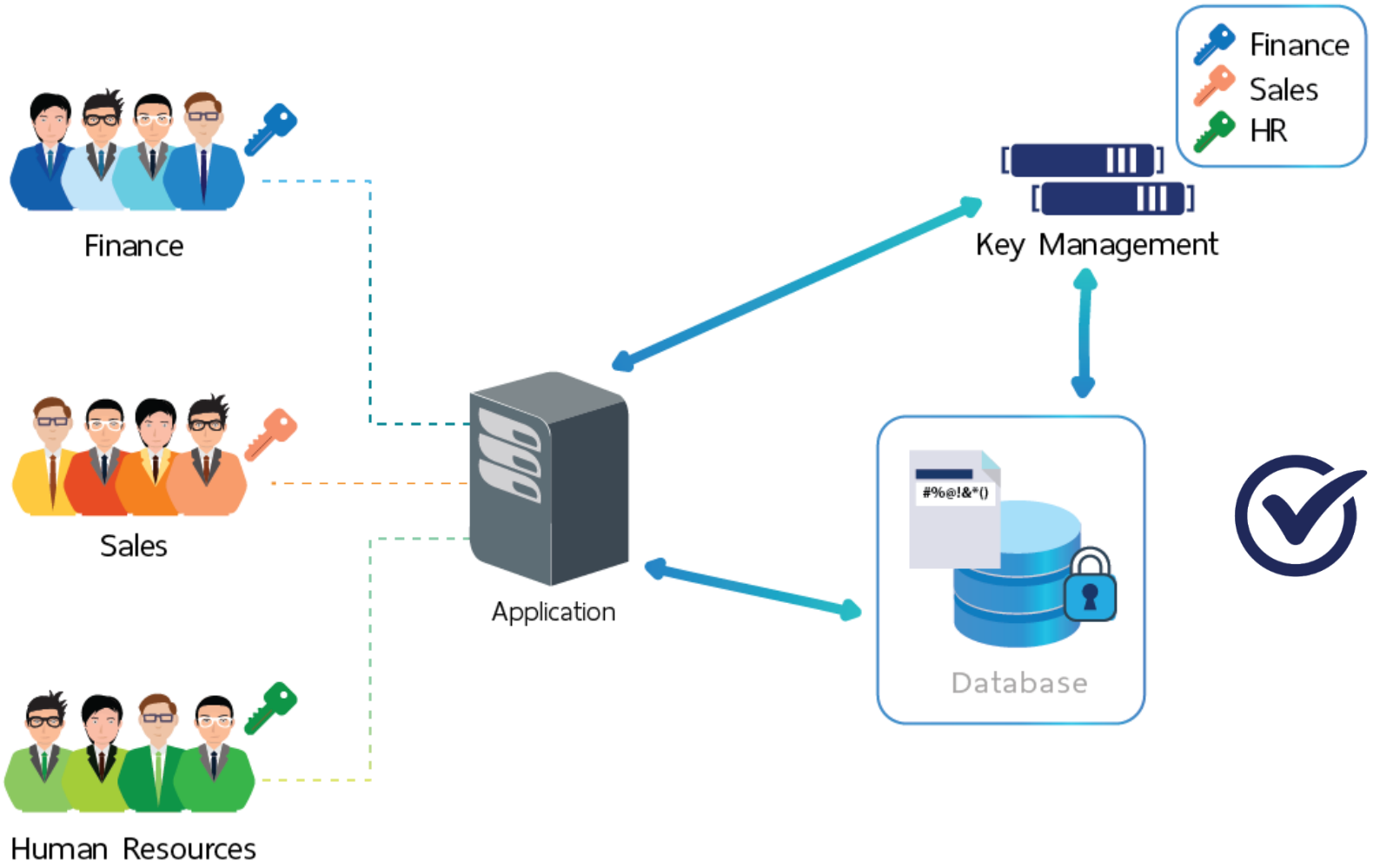
знаходить приховані загрози для бізнесу (DLP забезпечує швидкий та легкий для розуміння огляд усіх можливих загроз з єдиної консолі)

Ризики втрати корпоративної інформації



допомагає краще зрозуміти поведінку користувачів (створює звіти про усі операції з файлами, в тому числі їх відправлення через електронну пошту та друк. DLP також повідомляє про підозрілі дії та зміни в діяльності працівників)

Ризики втрати корпоративної інформації



визначає дані, які потребують найбільшої уваги (рішення DLP надає повну інформацію про те, хто, коли і де працював з конфіденційними файлами та як вони використовувались)

Рішення DLP

критерії оцінки продуктів DLP, сформульованих компанією Forrester Research:

- **перший критерій** - багатоканальність
- **другий критерій** - уніфікований менеджмент
- **третій критерій** - активний захист
- **четвертий критерій** - класифікація інформації з урахуванням, як вмісту, так і контексту

Кібер ризики підприємств

Цифровий ризик – це проблема бізнесу, а не лише технологічна проблема, тобто цифровий ризик відображає проблеми бізнесу загалом, а кіберризик – лише IT

Цифровий ризик-менеджмент, як наступна сходинка еволюції управління ризиком та безпеки підприємства, що широко використовує у своїй діяльності цифрові технології, має стосуватися компетенції топ-менеджменту, а не лише відділу IT

Кібер ризики підприємств

Цифровий ризик в умовах цифрової економіки

це економічна категорія, яка відображає особливості сприйняття суб'єктами економічних відносин об'єктивно існуючих невизначеності та конфліктності в процесах функціонування та управління компанією (організацією, підприємством тощо), що зумовлені можливими збоями у функціонуванні цифрових засобів і технологій, які використовуються компанією

Ризики, пов’язані з розвитком цифрової економіки

- загроза «цифровому суверенітету» країни, перегляд ролі держави в транскордонному світі цифрової економіки
- ризик кіберзагроз, пов’язаний із захистом персональних даних
- порушення приватного життя через потенційне спостереження за людьми
- загроза повноцінної «крадіжки особистості», тобто повноцінних цивільних і споживчих неправомірних дій та дій від імені іншої людини
- зниження рівня безпеки персональних даних

Ризики, пов’язані з розвитком цифрової економіки

- ризики штучного інтелекту, який при хакерських атаках легко доводить, що «він не робот», дозволяючи проводити різні несанкціоновані транзакції від імені суб’єкта господарювання
- «цифровий розрив» унаслідок цифрової нерівності використання сучасних цифрових технологій
- підвищення рівня складності бізнес-моделей і схем взаємодії
- різке посилення конкурентної боротьби в усіх сферах економіки та серйозні зміни в моделях поведінки виробників і споживачів
- необхідність перегляду адміністративного та податкового кодексів

Управління ризиком для підприємства

Політика управління ризиком для підприємства – це процес вироблення та реалізації програм, спрямованих на досягнення балансу між очікуваними вигодами від зменшення ризику у досягненні бажаного результату підприємницької діяльності та необхідними для цього витратами

Принципи формування політики управління господарськими ризиками:

- оптимальне співвідношення вигод та витрат
- максимум результату за прийнятного для підприємця ризику
- оптимальна ймовірність результату
- оптимальне коливання результату

Стратегія з управління ризиками

для прийняття рішень необхідно:

- дослідити ризики
- визначити мету реагування на ризики (рівень допустимого ризику)
- визначити обмеження щодо вибору засобів реагування (строки, ресурси, пріоритети (зовнішні та внутрішні))
- оцінити порівняльну ефективність заходів програми

дослідження ризиків включає два етапи:

- ідентифікація ризиків – процедури розпізнавання зовнішніх та внутрішніх для діяльності підприємства ризиків
- аналіз ризиків – процедури виявлення факторів ризиків та оцінки рівня їхньої значущості, аналіз ймовірності того, що відбудуться певні ризикові події та вплинуть на досягнення поставлених цілей

Методи проведення аналізу ризиків

- **побудова дерева рішень** – опис кожного етапу реалізації проєкту, з об’єктивною оцінкою ризиків, всіх витрат, а також ймовірних збитків та вигоди
- **аналоговий** – розробка нового проекту з урахуванням вже здійснених подібних проєктів
- **імітаційні методи** – виражаються у проведенні багаторазових дослідів з макетом, у якому проектуються пошуки значень ризиків покроково
- **експертний** – такий метод застосовний, якщо вихідних даних недостатньо, або немає, і тоді залучаються експерти для об’єктивної оцінки ризику

Методи проведення аналізу ризиків

- **ймовірнісний** – базуючись на статистичних даних, визначається ймовірність виникнення збитків, статистичні дані беруться за попередні періоди у певних зонах ризику
- **метод аналізу показників граничного рівня** – спрямований на визначення стійкості проекту до різноманітних факторів, здатних змінити умови реалізації даного проєкту
- **метод аналізу чутливості проєкту** – спрямований на об’єктивну оцінку значень впливу вихідних даних, що застосовуються під час розрахунків змін результатів проєкту
- **метод сценаріїв** – полягає у розробці кількох сценаріїв розвитку подій при реалізації проєкту та пропонується їх порівняльна оцінка

Методи проведення аналізу ризиків

Критеріїв вибору методів та методик для оцінки ризиків у діяльності підприємства малого бізнесу:

- метод повинен бути оптимальним за складністю, зрозумілим усім експертам, придатним для регулярного застосування
- має бути можливість адаптації методик оцінки ризиків до особливостей діяльності підприємства
- застосування методу має бути економічно доцільним з точки зору витрат на проведення аналітичних процедур
- для комплексної оцінки ризиків необхідно використання кількох методів оскільки більшість їх містить суб’єктивні елементи

Кіберризики: поняття та підходи

підходи щодо розуміння визначення кіберризику:

- причинно-наслідковий
- секторальний
- інструментальний

Кіберризик – це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб’єктами внаслідок їх функціонування у кіберпросторі

Джерела виникнення кіберризиків

Кіберризики розглядають в таких аспектах:

- систематичні ризики в діяльності фінансових установ та фінансових ринків
- складова операційних ризиків компаній
- ймовірності настання подій у сфері інформаційних активів, комп'ютерних та комунікаційних ресурсів
- ймовірні злочини, здійснені за допомогою мережі Інтернет

Форми кіберризиків:

- кібератака
- кіберінцидент
- кібертероризм
- кібервійна

Ознаки кібер-ризиків

- втрата або крадіжка носіїв інформації та мобільних пристроїв
- доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ
- ненавмисне розголошення співробітниками конфіденційної інформації
- навмисні дії співробітників (інсайдерів)
- неконтрольоване копіювання даних співробітниками

Види кібер-ризиків

- ризик втрати інформації під час злому паролю доступу або внаслідок DDoS-атаки
- ризик фінансових втрат від фішінгових атак
- ризик фінансових втрат через порушення роботи комп’ютерних систем
- ризик фінансових втрат від кібер-шантажу або вірусного блокування комп’ютерних систем
- ризик фінансових втрат через викрадення та розголошення персональних даних та інформації

Характеристика кіберризиків

Нецільові атаки

- **фішинг (вішинг, фармінг, клікфрода та ін.)** – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів
- **кардинґ** – вид шахрайства, при якому проводиться операція з використанням банківської картки або її реквізитів, яка не ініційована або не підтверджена її власником
- **смс-шахрайство** – вид шахрайства, при якому клієнту банку надсилають смс-повідомлення і/або телефонують з невідомого номера з метою отримання конфіденційної інформації по платіжній картці

Характеристика кіберризиків

Цільові атаки

- **фінансове шахрайство** – кримінологічне явище, що являє собою злочинну діяльність та виражається у системі кримінально-караних та легальних дій, які вчиняються шляхом обману або зловживання довірою в процесі формування, розподілу та використання грошових фондів з метою здобуття матеріальної вигоди

- **розкрадання баз даних** – характеризується незаконним обігом чужої сукупності даних, організованої відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами, в своїх корисливих інтересах або з корисливих мотивів в інтересах іншої особи

Характеристика кіберризиків

Цільові атаки

- **промислове шпигунство** – різновид економічного шпигунства, якому властиве звуження масштабів завдань з одержання інформації, що цікавить, від державного – до масштабу однієї або декількох фірм-конкурентів
- **DDoS атаки** – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена
- **кібервимагання (кріптолокери)** – вірусна атака, що включає в себе використання шкідливого програмного забезпечення (шкідливих програм), файли в якому зашифровані і робить їх непридатними для використання, до тих пір, поки викуп не буде оплачений

Характеристика кіберризиків

Атаки зсередини

- **навмисна шкода та розкрадання інформації** – несанкціоноване копіювання інформації, збій IT-інфраструктури, втрата переносних пристроїв, відправка «не тих» даних, поширення конференційної інформації за допомогою соціальних мереж, надання неякісних послуг з аутсорсингу (хмарні сервіси, дата-центри, колл-центри тощо)
- **знищення інформації** – послідовність операцій, призначених для здійснення програмними або апаратними засобами безповоротного видалення даних, у тому числі залишкової інформації
- **сприяння цільової атаці** – підтримка атак «замовного» характеру, спеціально націленої на один сайт або їх групу, що об'єднані однією ознакою

Кіберризики

Для мінімізації або усунення кіберризиків існує три основних напрямки:

- технологічні рішення безпеки
- просвітницька робота в сфері протидії та профілактики кіберзлочинів
- кіберстрахування

Робота з ризиками

підходи до роботи з кіберзагрозами

- **Avoid** (піти від ризику) – це оптимізація бізнес-процесів таким чином, щоб не використовувати дані, втрата яких стане критичною для компанії
- **Except** (якщо кібер-ризик має невеликий вплив на бізнес) - приймаєте таку вірогідність та продовжує працювати без зміни бізнес-підходів
- **Mitigation** (пом'якшення кібер-ризиків та їх впливу на компанію) - проведення аудиту та визначення, наскільки є вразливою ваша IT-архітектура перед хакерами
- **Transfer** (передача відповідальності за кібер-ризик). Передача команді або компанії (аутсорсинг) відповідальність за питання кібербезпеки бізнесу

Управління кібер-ризиками

передумов для формалізації процесів управління кібер-ризиками

- оцифровка (або «діджіталізація») сучасного бізнесу (практично не залишилося галузей, які не залучені в кіберпростір, і розмір компаній вже також не має значення)
- потрапляння самої людини до охоплення застосування кібер-ризиків (людина навіть сама по собі вже є інформаційним активом, який необхідно захищати)
- зростання залежності областей безпеки одна від одної (наприклад, фізичної безпеки від інтернету речей)
- потреба топ-менеджерів у простому й зрозумілому інструменті оцінки безпеки та її розвитку

Сервіси пошуку інформації про юридичних та фізичних особам

Верховна Рада України
Законодавство України

Державна реєстрація юридичних осіб та фізичних осіб-підприємців здійснюється відповідно до Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань»

https://zakon.rada.gov.ua/laws/show/755-15#Text

Сервіси пошуку інформації про юридичних та фізичних особам

Відомості з реєстру бізнесу

- надання відомостей з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань

Відомості з реєстру банкрутства

- отримання відомостей з Єдиного реєстру підприємств, щодо яких порушено провадження у справі про банкрутство

Сервіси пошуку інформації про юридичних та фізичних особам

Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань

- публічний реєстр юридичних осіб в Україні, виконує роль державного контролю та захисту прав юридичних осіб, громадських формувань та підприємців України, а також захисту прав третіх осіб у правовідносинах з ними

Єдиний державний реєстр підприємств та організацій України

- статистичний реєстр підприємств в Україні, автоматизована система збирання, накопичення та обробки даних про підприємства та організації усіх форм власності, а також їх відокремлені підрозділи - філії, відділення, представництва тощо

Сервіси пошуку інформації про юридичних та фізичних особам

Єдиний реєстр ліцензій

- дозволяє переконатися в наявності ліцензії у компанії, з якою плануєте співпрацювати або навпаки – дізнатися про відсутність дозвільних документів

Єдиний державний реєстр судових рішень

- автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень

Сервіси пошуку інформації про юридичних та фізичних особам

YouControl

https://youcontrol.com.ua/

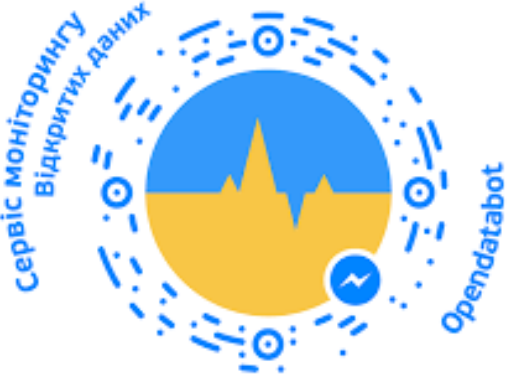
аналітична онлайн-система

- допомагає комплексно оцінювати контрагентів різним спеціалістам компанії
- перевіряти контрагентів та стежте за їх змінами

Сервіси пошуку інформації про юридичних та фізичних особам

Опендатабот

opendatabot.ua



- спосіб перевіряти компанії та людей на iOS, Android, Telegram та Viber
- доступ до державних реєстрів: ЄДР, РРП, ЄРСР, ДРОРМ, АСВП/ЄРБ в режимі реального часу

Сервіси перевірки інформації про контрагентів

«CONTR AGENT» та «VERDICTUM» від ЛІГА:ЗАКОН

https://ca.ligazakon.net/

- Аналіз та моніторинг контрагента у режимі 24/7 та своєчасне інформування про зміни
- Актуальна та достовірна інформація з державних реєстрів та відкритих джерел
- Відображення ризик-факторів контрагента - від статусу банкрутства до санкцій
- Виявлення усіх можливих зв’язків компанії та персон за допомогою machine learning

Сервіси перевірки інформації про контрагентів

YouControl - аналітичний сервіс для ділової розвідки та перевірки контрагентів

https://youcontrol.com.ua/

opendatabot.ua

Опендатабот - отримання інформації про будь-яку організацію чи підприємство України

ДОДАТКОВІ РЕСУРСИ

- Опендатабот
- Корпоративна та персональна цифрова безпека під час війни - поради і корисні посилання
- Кібергігієна: безпека для людей і бізнесів

Цифрова безпека бізнесу та кібер ризики підприємств в умовах цифрової економіки

- Запитання
- Ідеї
- Обговорення