Загальна (сертифікована) короткострокова програма
«Інформаційна безпека та кібербезпека в органах влади»

Тема:
Основи інформаційної безпеки

Артем СЕРЕНОК

к.держ.упр., доцент кафедри цифрових технологій та е-урядування ННІ "Інститут державного управління" ХНУ ім. В.Н. Каразіна
тренер з відкритих даних Національної мережі тренерів з відкритих даних
Національний консультант у сфері е-урядування в Донецькій області від ПРООН в Україні

Структура загальної (сертифікованої) короткострокової програми (дистанційно) «Інформаційна безпека та кібербезпека в органах влади»

- Основи інформаційної безпеки
- Інститути й інструменти забезпечення інформаційної безпеки України
- Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки
- Кіберзлочинність
- Безпека електронних платіжних систем
- Безпека роботи в Інтернет
- Соціальна інженерія
- Безпека мобільних пристроїв
- Захист інформації в мережах. Захист персональних даних

Понятійно-категорійний апарат

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Доктрина інформаційної безпеки України *(Затверджено Указом Президента України від 8 липня 2009 року N 514/2009)*

Понятійно-категорійний апарат

Ідентифікація - процедура розпізнавання суб'єкта по його ідентифікатору

Аутентифікація - процедура перевірки автентичності суб'єкта, що дозволяє переконатися в тому, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує

Авторизація - процедура надання суб'єкту певних прав доступу до ресурсів системи

Загроза - це потенційно можлива подія, неважливо, навмисна чи ні, яка може небажано вплинути на систему, а також на інформацію, що зберігається в ній

Вразливість - це деяка невдала характеристика системи, яка робить можливим виникнення загрози

Атака - це дія, що виконується зловмисником, яка полягає в пошуку і використанні тієї або іншої вразливості для реалізація загрози

Експлоїт - комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують вразливості і застосовуються для здійснення атак

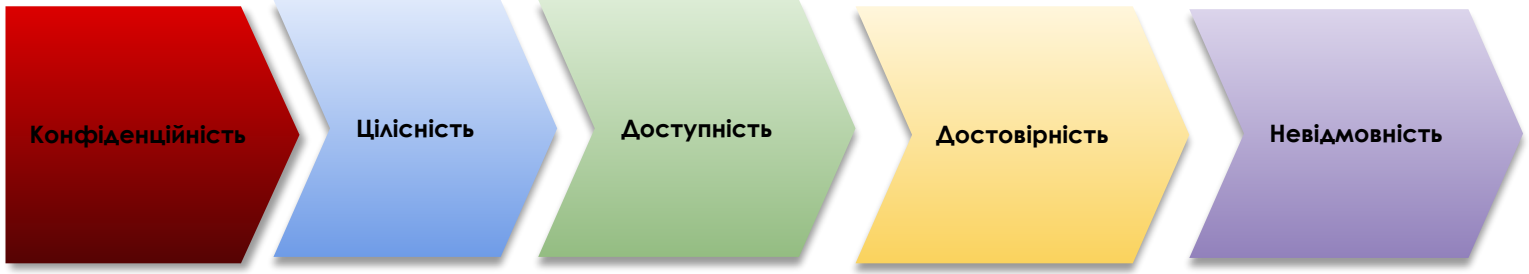
Властивості (елементи) інформаційної безпеки

Властивості (елементи) інформаційної безпеки

Гарантія того, що інформація доступна тільки для авторизованих користувачів

Гарантія того, що система, відповідальна за доставку, зберігання і обробку інформації доступна, у момент запиту авторизованим користувачем

Гарантує, що відправник повідомлення не може пізніше заперечувати факт відправки повідомлення і що одержувач не може заперечувати факт його отримання

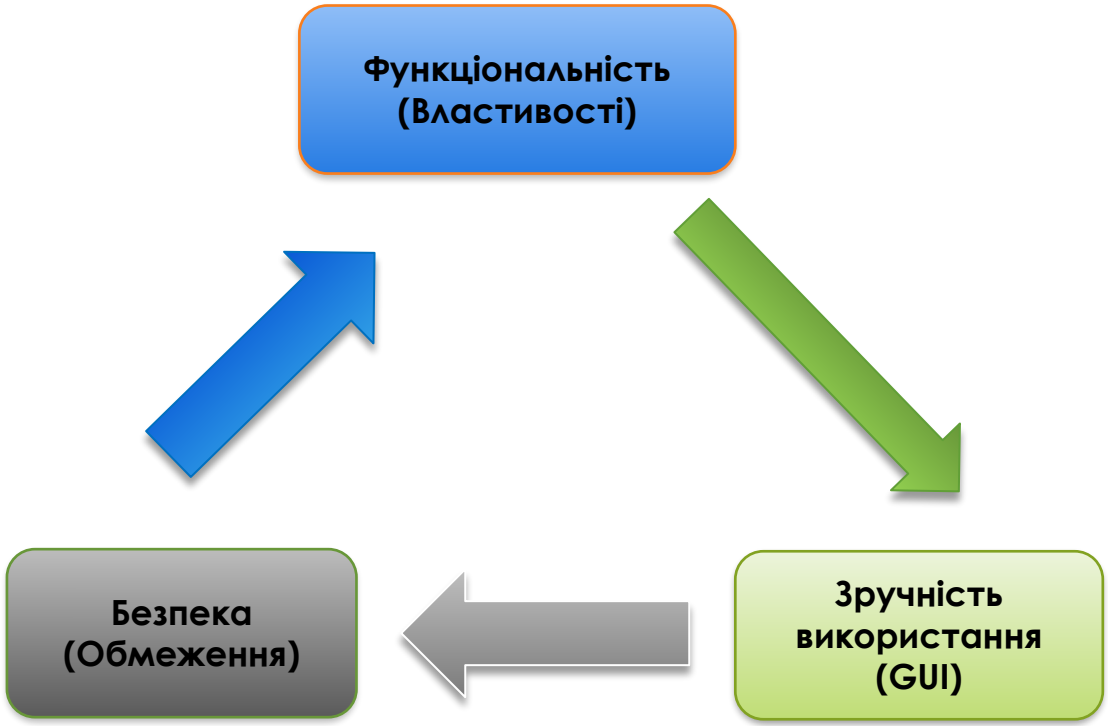


Запобігання зміни інформації неавторизованими користувачами

Характеризує ступінь автентичності інформації (відсутність відмінностей від оригіналу)

Трикутник безпеки, функціональності і зручності використання

Рівень безпеки у будь-якій системі може бути визначений співвідношенням трьох компонент:



Інформаційна безпека
Вектори атаки

Загрози інформаційної безпеки

Загрози мережі

- Збір інформації;
- Сніффінг і підслуховування;
- Підміна параметрів;
- Перехоплення сеансу і атака «Людина посередині»;
- SQL-ін'єкції;
- Отруєння ARP;
- Атаки перебором паролів;
- Атака «Відмова в обслуговуванні»

Загрози вузла

- Шкідливе ПЗ;
- Збір інформації про вузол;
- Атаки, засновані на паролі;
- Довільне виконання коду;
- Несанкціонований доступ;
- Підвищення привілеїв;
- Бекдор атаки;
- Загрози фізичної безпеки

Загрози застосування

- Проблеми контролю введення даних;
- Атаки аутентифікації та авторизації;
- Управління конфігурацією;
- Розкриття інформації;
- Проблеми управління сеансами;
- Проблеми переповнення буфера;
- Криптографічні атаки;
- Зміна параметрів застосувань;
- Неправильна обробка помилок;
- Проблеми аудиту та журналювання дій

Фази злому

- Розвідка відноситься до підготовчої фази, коли хакер виконує збір інформації про цілі
- У разі отримання нових знань про цілі, може вимагати його повторити
- Метою цього етапу є: клієнти і персонал організації, інформація про мережу і про операційні системи

Типи розвідки

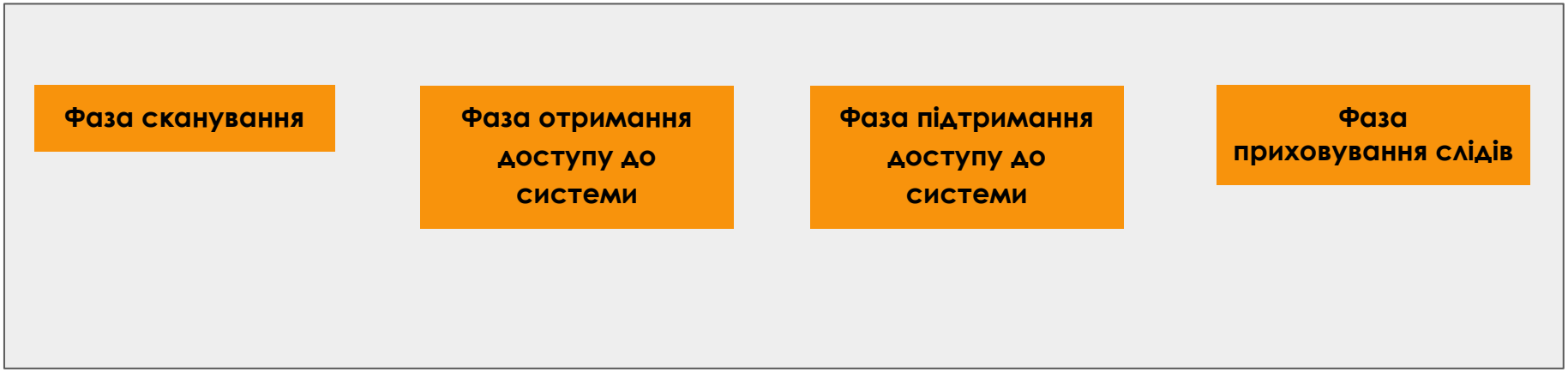
Пасивна розвідка

- Пасивна розвідка використовує отримання інформації без прямої взаємодії з ціллю
- Наприклад, пошук публічних записів або випусків новин

Активна розвідка

- Активна розвідка використовує пряму взаємодію з ціллю
- Наприклад, телефонні дзвінки до техпідтримки або технічного відділу

Фази злому


Фаза сканування
Фаза отримання доступу до системи
Фаза підтримання доступу до системи
Фаза приховування слідів

Фази злому (продовження)

- **Фаза сканування**
  - Зловмсник сканує мережу для пошуку певної інформації на базі інформації зібраної під час розвідки
  - **Сканування портів**
  - Цей етап може включати використання сканерів портів, утиліт для побудови карти мережі, утиліт на базі протоколу ICMP, сканерів вразливостей і так далі
  - **Витягання (перерахування) інформації**
  - Зловмисник витягає таку інформацію: активні вузли, порти і їх статус на активних вузлах, деталі ОС, типи пристроїв, час роботи системи і так далі

Фази злому (продовження)

- **Фаза отримання доступу до системи**
    - Точка, в якій зловмисник отримав доступ до операційної системи або застосування на комп'ютері або в мережі.
    - Зловмисник може підвищити привілеї облікового запису для отримання повного контролю над системою.
    - Дії, які може виконувати зловмисник на цьому етапі: злом паролів, переповнення буфера, атака відмова в обслуговуванні, перехоплення сесій і т.д.

Фази злому (продовження)

- **Фаза підтримання доступу до системи**
  - Зловмисник намагається зробити систему недоступною для злому іншими зловмисниками, захищаючи свій ексклюзивний доступ через бекдори, руткіти або трояни.
  - Зловмисник може завантажувати, викачувати або маніпулювати даними, застосуваннями або конфігурацією зламаної системи.
  - Зловмисник може використовувати скомпрометовану систему для наступних атак.

Фази злому (продовження)

- **Фаза приховування слідів**
  - Приховування слідів відноситься до діяльності, якою займається зловмисник для приховування своїх дій.
  - Наміри зловмисника включають: підтримку доступу до системи жертви, залишаючись непоміченим і не спійманим, тому необхідно видалити докази, які можуть призвести до його розкриття

Типи атак

- Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі:
  - порушення конфіденційності переданої інформації;
  - порушення цілісності та достовірності інформації, що передається;
  - порушення працездатності системи в цілому або окремих її частин.

Типи атак

Атаки на операційну систему

Отримання доступу

- Зловмисники шукають вразливості в операційній системі або її налаштуваннях і використовують їх для отримання доступу до вузла

Вразливості ОС

- Вразливості переповнення буфера
- Помилки в коді компонент операційної системи
- Операційна система з не встановленими оновленнями

Атаки на ОС

- Використання специфічних реалізацій протоколів
- Атака на вбудовану систему аутентифікації
- Злом безпеки файлової системи
- Злом паролів і механізмів шифрування

Атаки на неправильну конфігурацію

Неправильне налаштування прав доступу до файлів або до інших системних ресурсів

Невикористовувані сервіси, що поставляються разом з операційною системою або додатками

Використання налаштувань за замовчуванням для мережних пристроїв або мережних сервісів

Атаки рівня застосувань

Зловмисник може використовувати вразливості в застосуваннях, запущених в інформаційній системі організації для отримання несанкціонованого доступу

Слабка або відсутня перевірка на помилки в застосуваннях веде до:

- Атаки переповнення буфера
- Розкриттю конфіденційної інформації
- Використанню міжсайтового скриптінга
- Перехопленню сесій і атаці «Людина посередині»
- Атаки «Відмова в обслуговуванні»
- Атаки SQL-ін'єкцій

Інші атаки рівня застосувань включають:

- Фішинг
- Підробка параметрів / форм
- Атаки на посилання між каталогами

Багатошаровий захист

- **Багатошаровий захист** – це стратегія безпеки, в якій кілька захисних шарів розміщені через всю інформаційну систему.
- Допомагає уникнути прямих атак проти інформаційної системи і даних, оскільки злом одного шару призводить зловмисника тільки до наступного рівня.

Політики інформаційної безпеки

- Політика безпеки є основою інфраструктури безпеки
- Політика безпеки - це документ або набір документів, який описує управління безпекою, яка реалізована в організації

Цілі політик безпеки

- Підтримка плану для управління та адміністрування мережною безпекою
- Захист комп'ютерних ресурсів організації
- Розділення прав доступу користувачів
- Захист конфіденційної інформації від крадіжок, зловживань, неавторизованого розкриття
- Уникання неавторизованих модифікацій даних
- Зменшення ризиків, викликаних нелегальним використанням системних ресурсів організації

Дослідження вразливостей

- Процес дослідження вразливостей і помилок проектування, який відкриває операційну систему і її застосування для атаки або зловживання
- Вразливості класифікуються на основі рівня строгості (низький, середній, високий) і ранг використання (локально або віддалено)

Адміністратор повинен для пошуку вразливостей:

Збирати інформацію про тенденції, вразливості і загрози безпеці

Шукати вразливості до моменту виконання атаки

Отримувати інформацію, яка допоможе уникнути проблем з безпекою

Знати як відновити систему після атаки

Тестування на проникнення

- Тестування на проникнення - це метод оцінки інформаційної безпеки системи або мережі симуляцією атаки для пошуку вразливостей, які може використовувати зловмисник
- Тестування включає активний аналіз конфігурації системи, пошук недоліків проектування, архітектури мережі, технічних недоліків і вразливостей
- Тестування методом «чорний ящик» симулює атаку від когось, у кого немає яких-небудь знань про систему, тестування методом «білий ящик» симулює атаку від когось, хто має повні знання про систему
- Комплексний звіт з деталями знайдених вразливостей і набір рекомендованих контрзаходів доставляється замовнику

Дякую за увагу