Урок № 7

Тема. Основні захисні механізми які реалізуються в рамках різних заходів. Ідентифікація та аутендифікація користувачів

Мета:

- ✔ ***навчальна:*** ознайомитися з методами, що забезпечують санкціонованим особам доступ до об'єктів АС - авторизація, ідентифікація, аутендифікація, їх різновидами;
- ✔ ***розвиваюча:*** розвивати логічне й алгоритмічне мислення; формувати вміння діяти за інструкцією, планувати свою діяльність, аналізувати і робити висновки;
- ✔ ***виховна:*** виховувати інформаційну культуру учнів, уважність, акуратність, дисциплінованість.

Обладнання: комп'ютери кабінету з виходом в мережу Інтернет, мультимедійний проектор, презентація уроку, електронні матеріали.

Тип уроку: урок засвоєння нового матеріалу.

ХІД УРОКУ.

I. Організація класу до уроку

1) Привітання із класом

II. Перевірка домашнього завдання. Актуалізація опорних знань

1) Словник інформаційної безпеки (учні зачитують знайдені відповіді):
   - ФРІКЕР – людина, що займається зламом телефонних, мереж мобільних операторів з метом здійснення безкоштовних дзвінків, поповнення особистого мобільного рахунку.
   - КАРДЕР - Люди, які крадуть гроші з банківських карт,
   - ІНСАЙДЕР (insider) – особа, яка має доступ до конфіденційної інформації та може використати її у власних цілях з метою збагачення, одержання неконкурентних переваг, привілеїв тощо.
   - СПАМЕР – людина, що розсилає спам,
   - СКРИПТ-КІДДІ – скриптові дітки, або кулхакери (експериментатори)
2) Компютерне тестування– Урок 6 (Mytest)

Мотивація навчання

Ми вже знаємо, що засоби і методи захисту інформації зазвичай ділять на дві великі групи: організаційні та технічні. Під *організаційними* маються на увазі законодавчі, адміністративні та фізичні, а під *технічними* - апаратні, програмні і криптографічні заходи, спрямовані на забезпечення захисту об'єктів, людей та інформації.

Сьогодні ми ознайомитися з методами, що забезпечують санкціонованим особам доступ до об'єктів АС, дізнаємося, що таке ідентифікація, аутентифікація, авторизація і в чому різниця між цими поняттями

IV. Вивчення нового матеріалу

Пояснення вчителя з елементами демонстрування презентації

(використовується проектор)

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами.

Під НСД мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розуміються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін.

Захист від НСД може здійснюватися в різних складових інформаційної системи: на прикладному і програмному рівні, на апаратному та на мережевому рівні.

Для захисту інформації на рівні прикладного та системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації;
- системи аудиту та моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються: апаратні ключі; системи сигналізації; засоби блокування пристроїв та інтерфейс вводу-виводу інформації.

Розглянемо методи, що забезпечують санкціонованим особам доступ до об'єктів та інформаційних ресурсів. До них відносять аутентифікацію та ідентифікацію користувачів.

Аутентифікація - це метод незалежного від джерела інформації встановлення автентичності інформації на основі перевірки достовірності її внутрішньої структури ("це той, ким назвався?").

Авторизація - в інформаційних технологіях це надання певних повноважень особі або групі осіб на виконання деяких дій в системі обробки даних. ("Чи має право виконувати цю діяльність?"). За допомогою авторизації встановлюються і реалізуються права доступу до ресурсів.

Ідентифікація - це метод порівняння предметів або осіб за їх характеристиками, шляхом розпізнавання з предметів або документів, визначення повноважень, пов'язаних з доступом осіб в приміщення, до документів і т.д. ("Це той, ким назвався і має право виконувати цю діяльність?").

Що таке ідентифікація?

Ідентифікація - посвідчення або підтвердження автентичності особи або будь-якої інстанції при їх зверненні до захищеної обчислювальної системи, забезпечує перевірку достовірності партнерів по спілкуванню і перевірку достовірності джерела даних

Ідентифікація - це процедура розпізнавання суб'єкта за його ідентифікатором (простіше кажучи, це визначення імені, логіна або номера).

Ідентифікація виконується при спробі увійти в будь-яку систему (наприклад, в операційну систему або в сервіс електронної пошти). Мета ідентифікації — перевірити, чи відомий індивід системі. Ідентифікатором може бути: номер телефону, номер паспорта, e-mail, номер сторінки в соціальній мережі і т.д.

Коли нам дзвонять з невідомого номера, що ми робимо? Запитуємо "Хто це", тобто дізнаємося ім'я. Ім'я в даному випадку і є *ідентифікатор*, а відповідь вашого співрозмовника - це буде *ідентифікація*.

Що таке аутентифікація?

Після ідентифікації проводиться аутентифікація - це процедура перевірки автентичності (перевірка справжності). Це процес розпізнавання користувача системи і надання йому певних

прав та повноважень. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає.

Аутентифікація (authentification) - це процес перевірки облікових даних користувача (зазвичай імені та пароля). Іншими словами введені облікові дані звіряються з даними, що зберігаються в базі даних (користувача перевіряють за допомогою пароля, лист перевіряють по електронного підпису і т.д.)

Способи Автентифікації

- ✔ Парольна (здійснюється на основі володіння користувачем певної конфіденційної інформації)
- ✔ Біометрична (основана на унікальності певних антропометричних характеристик людини)

Щоб визначити чиюсь справжність, можна скористатися трьома факторами:

- **Пароль** - то, що ми знаємо (слово, PIN-код, код для замка, графічний ключ): об'єкт може продемонструвати знання якого-небудь загального для сторін секрету
- **Пристрій** - то, що ми маємо (пластикова карта, ключ від замка, USB-ключ)
- **Біометрика** - то, що є частиною нас (відбиток пальця, портрет, сітківка ока)

Парольна аутентичність

Більшість мережевих систем на даний час продовжують використовувати парольну аутентифікацію, оскільки вона простіше і дешевше. Перевірка автентичності користувача звичайно здійснюється операційною системою. Користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль.

Конструкція пароля: Для розумної ефективності паролі повинні складатися не менше ніж з 6-8 символів, не бути легко згадувані і змінюватися не рідше, ніж кожні 90 днів.

Чим довше пароль, тим більше складнощів для зловмисника, щоб його вгадати або обчислити. Можна стверджувати, що збільшення довжини пароля тільки на один символ помітно збільшує безпечний час: якщо очікуваний безпечний час для пароля з трьох символів становить близько трьох місяців, безпечний час для пароля з чотирьох символів становить сімдесят вісім місяців.

Так само важлива форма пароля. Користувач повинен бути в змозі впевнено його пам'ятати (і не відчувати незручностей від неможливості його записувати), але пароль також повинен бути дуже складним для вгадування іншими. Телефонний номер шкільної подруги або назва вулиці – приклади правильних форм.

Біометрична аутентифікація

Системи біометричного захисту використовують унікальні для кожної людини вимірювані характеристики для перевірки особи індивіда.

Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів.

До біометричних засобів захисту інформації відносять системи аутендифікації за:

- ✔ Параметрами голосу.
- ✔ Візерунком райдужної оболонки ока і карта сітчатки ока.
- ✔ Рисами обличчя.
- ✔ Формою долоні.
- ✔ Відбитками пальців.
- ✔ Формою і спосібом підпису.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення.

Для того, щоб біометрична система змогла надалі аудентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Під час процедури реєстрації в базу даних системи заносяться характеристики користувачів, необхідні для встановлення їх автентичності.

Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і виносять рішення, хто постав перед сканером.

- **Аутентифікація по райдужній оболонці ока**

Райдужна оболонка ока є унікальною для кожної людини біометричної характеристикою. Зображення ока виділяється з зображення особи і на нього накладається спеціальна маска штрих-кодів. Результатом є матриця, індивідуальна для кожної людини.

- **Аутентифікація по зображенню особи**

Для ідентифікації особи часто використовуються технології розпізнавання по обличчю. Розпізнавання людини відбувається на відстані. Ідентифікаційні ознаки враховують форму особи, його колір, а також колір волосся. До важливих ознак можна віднести також координати точок особи в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал).

Алгоритм функціонування системи розпізнавання: Зображення особи зчитується звичайною відеокамерою і аналізується. Програмне забезпечення порівнює введений портрет з еталоном, що зберігаються. Важливо також те, що біометричні системи цього класу здатні виконувати безперервну аутентифікацію користувача комп'ютера протягом всього сеансу його роботи

- **Аутентифікація по долоні руки.**

У біометриці з метою ідентифікації використовується проста геометрія руки - розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин). Сканери ідентифікації по долоні руки встановлені в деяких аеропортах, банках і на атомних електростанціях.

Метод розпізнавання геометрію кисті руки заснований на аналізі тривимірного зображення кисті. Однак форма кисті руки також є параметром, який досить сильно схильний до змін в часі, а крім того, вимагає сканерів великого розміру, що веде до подорожчання системи

- **Аутентифікація за відбитками пальців**

Оптичні сканери зчитування відбитків пальців встановлюються на ноутбуки, миші, клавіатури, флеш-диски, а також застосовуються у вигляді окремих зовнішніх пристроїв і терміналів (наприклад, в аеропортах і банках) .Якщо візерунок відбитка пальця не збігається з візерунком допущеного до інформації користувача, то доступ до інформації неможливий

- **Аутентифікація по характеристикам мови**

Ідентифікація людини по голосу - один з традиційних способів розпізнавання, інтерес до цього методу пов'язаний і з прогнозами впровадження голосових інтерфейсів в операційні системи.

Що таке авторизація? Коли визначили ідентифікатор, перевірили справжність, вже можна надавати і доступ, тобто, виконати авторизацію. **Авторизація** - це надання доступу до будь-якого ресурсу (наприклад, до електронної пошти).

- **Чим відрізняється авторизація від аутентифікації?**

Ідентифікація – це процедура розпізнавання суб'єкта за його ідентифікатором. Мета **аутентифікації** — перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а **авторизація** полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи, тобто після аутентифікації.

Автентифікація — це процес доказу об'єктом своєї дійсності системі.

Ідентифікація — це процес визначення прав об'єкта стосовно системи.

Авторизація — це процес доказу дій об'єкта стосовно системи або інших об'єктів.

Засоби ідентифікації й авторизації часто реалізуються в одній підсистемі. Перші дозволяють визначити приналежність того чи іншого ресурсу мережі об'єкта, а другі реалізують механізм причетності, у результаті чого об'єкт не зможе довести, що не робив спроби обігу або впливу на ресурс. Такі засоби контролюють доступ об'єктів до ресурсів системи, надаючи кожному об'єкту саме ті права, які йому були визначені відповідальною особою.

IV. Формування практичних умінь і навичок

Увага! ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

Завдання 1. Ознайомитися з основними правилами кіберзахисту та правилами створення надійного пароля на сайті https://cyberukraine.in.ua/ (#ПарольГраєРоль)

Завдання 2. Здійсніть перевірку пароля на сайті Проверка пароля - Zillya! https://zillya.ua/ru/check-password

Обговорюємо .

1. Вкажіть переваги і недоліки біометричної системи захисту даних
2. Чому біометричні системи захисту інформації є найбільш надійними?
3. Як ви думаєте, які недоліки ідентифікації людей за характеристиками голосу? Наведіть приклади застосування даного методу ідентифікації.
4. Чому райдужка краще за інших біометрічних технологій?
5. Вкажіть проблеми ідентифікації особистості по обличчю.

Працюємо в парах. Які умови дозволяють не встановлювати пароль на комп'ютері?

V. Підсумок уроку

Рефлексія

- *Що нового сьогодні дізналися? Чого навчилися?*
- *Що сподобалось на уроці, а що ні? Чи виникали труднощі?*

VI. Домашнє завдання

1) Опрацювати **конспект**, знайти означення та пояснити термін "двоетапна аутентифікація»
2) За матеріалами Інтернету підготуйте бюлетень "Як придумати надійний пароль і де його зберігати". Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів