Урок № 8

Тема. Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем. Реєстрація та оперативне оповіщення про події безпеки. Криптографічні методи захисту інформації.

Мета:

- ✓ ***навчальна:*** дати уявлення про розмежування доступу, криптографічні методи захисту інформації та про контроль цілісності інформаційних ресурсів; ознайомити з основними методами крипто логічного захисту та з відомими алгоритмами шифрування; сформувати навички застосування найпростіших криптографічних шрифтів;
- ✓ ***розвиваюча:***розвивати логічне й алгоритмічне мислення, творчу ініціативу та активність; формувати вміння діяти за інструкцією, планувати свою діяльність, аналізувати і робити висновки;
- ✓ ***виховна:*** виховувати інформаційну культуру учнів, уважність, акуратність, дисциплінованість.

ХІД УРОКУ.

Найбільший збиток інформації та інформаційних систем наносять неправомірні дії співробітників і комп'ютерні віруси. Для захисту інформації в комп'ютерах та інформаційних мережах широко використовуються різноманітні засоби захисту. Вони включають різні системи обмеження доступу до об'єкту. Їх мета - найбільшою мірою утруднити чи унеможливити реалізації загроз безпеки.

Сьогодні ми ознайомимося з поняттям розмежування доступу, криптографією та її різновидами.

Вивчення нового матеріалу

Контроль доступу - це процес захисту даних і програм від їх використання об'єктами, які не мають на це права. Щоб контроль доступу був ефективним, необхідно забезпечити засоби аутентифікації кожного користувача.

Правила розмежування доступу (access mediation rules) — найважливіша частина політики безпеки, що регламентує правила доступу користувачів і процесів до ресурсів інформаційної сфери.

Під **розмежуванням доступу** прийнято розуміти встановлення повноважень суб'єктів з метою наступного контролю санкціонованого використання ресурсів доступних в системі.

Простіше кажучи**, розмежування доступу** полягає в тому, щоб кожному зареєстрованому користувачу надати можливості безперешкодного доступу до інформації в межах його повноважень і виключити можливості перевищення цих повноважень.

Розмежування доступу зареєстрованих користувачів до інформаційних ресурсів здійснюється системами захисту інформації відповідно до встановлених для користувачів повноважень. Повноваження користувачів встановлюються за допомогою спеціальних налаштувань системи. По відношенню до інформаційних ресурсів засобами захисту можуть встановлюватися такі повноваження, як дозвіл читання, запису, створення, запуску виконуваних файлів і інші.

Розмежування може здійснюватися:

- ***за рівнями таємності*** (секретно, цілком таємно і т.п.). Користувачеві дозволяється доступ тільки до даних свого або більш низьких рівнів. Захищаються дані розподіляються по масивах таким чином, щоб в кожному масиві містилися дані одного рівня таємності;
- ***спеціальними списками***. При цьому розмежування доступу для кожного елемента даних, що захищаються (файлу, програми, бази) складається список всіх тих користувачів, яким надано право доступу до відповідного елементу. Можливий зворотний варіант, коли для кожного зареєстрованого користувача складається список тих елементів даних, що захищаються, до яких йому надано право доступу;

- ***матрицями повноважень***.

При *організації доступу* до обладнання істотне значення мають ідентифікація і аутентифікація користувачів, а також контроль і автоматична реєстрація їх дій. Для впізнання користувача можуть бути використані паролі і індивідуальні ідентифікаційні картки, а для управління доступом до устаткуванню такі прості, але ефективні заходи, як відключення живлення або механічні замки і ключі для пристроїв.

Система розмежування доступу до програм і даних повинна містити 4 функціональні блоки:

- блок ідентифікації і аутентифікації суб'єктів доступу;
- диспетчер доступу, реалізується у вигляді апаратно-програмних механізмів і забезпечує необхідну дисципліну розмежування доступу суб'єктів до об'єктів доступу (у тому числі і до апаратних блоків, вузлів, пристроїв);
- блок криптографічного перетворення інформації при її зберіганні і передачі;
- блок очищення пам'яті.

Прийнято виділяти два основні **методи розмежування доступу**: дискреційне і мандатне.

Дискреційним називається розмежування доступу між названими суб'єктами (користувачами) і поіменованими об'єктами (файли, програми тощо) відповідно до матриці доступу.

Мандатне розмежування доступу зазвичай реалізується як розмежування доступу за рівнями секретності: кожному суб'єкту і кожному об'єкту призначаються класифікаційні мітки, що відображають їх рівень.

Принципова відмінність між дискреційним і мандатним розмежуванням доступу полягає в наступному: якщо у разі дискреційного розмежування доступу права на доступ до ресурсу для користувачів визначає його власник, то у разі мандатного розмежування доступу рівні секретності задаються ззовні, і власник ресурсу не може здійснювати на них вплив. Сам термін «мандатне» є поверхневою інтерпретацією слова mandatory – «обов'язковий». Тим самим, мандатне розмежування доступу слід розуміти як примусове.

Основи криптографії

Одним з найбільш відомих способів захисту інформації є її кодування (шифрування, криптографія). Воно не рятує від фізичних впливів, але в решті випадків служить надійним засобом.

Криптографія – це прикладна наука, яка використовує найсучасніші досягнення фундаментальних наук і, в першу чергу, математики. З іншого боку, всі конкретні завдання криптографії істотно залежать від рівня розвитку техніки і технології, від застосовуваних засобів зв’язку і способів передавання інформації. Розвинулась дана наука з практичної потреби передавати важливі відомості найнадійнішим чином.

Криптографія (від грецького kryptos - прихований і graphein - писати) - наука про математичні методи забезпечення конфіденційності і автентичності інформації.

Криптографія займається методами перетворення інформації, які б не дозволили зловмиснику витягти її з повідомлень, що перехоплюються. При цьому по каналу зв’язку передається вже не сама інформація, що захищається, а результат її перетворення за допомогою шифру, і для зловмисника виникає складне завдання розкриття шифру.

Тобто, криптографія повинна забезпечити такий захист інформації, що навіть у випадку її перехоплення сторонніми особами й обробки будь-якими способами з використанням комп’ютерів і останніх досягнень науки і техніки вона не повинна бути дешифрована протягом декількох десятків років.

Вона вважається потужним засобом забезпечення конфіденційності і контролю цілісності інформації. Поки альтернативи методам криптографії немає

В криптографії застосовуються такі поняття:

Зашифрування **–** це процес перетворення інформації, при якому її зміст стає незрозумілим для суб’єктів, що не мають відповідних повноважень

Результат зашифрування інформації називають *шифротекстом* або *криптограмою*.

Розшифрування - процес перетворення зашифрованої інформації у придатну для читання інформацію.

Сукупність процесів зашифрування і розшифрування називають *шифруванням.*

Відкритий текст - початкове повідомлення, яке повинен захистити криптограф.

Кодування - заміна логічних (смислових) елементів, наприклад, слів.

Дія криптографії

Криптографічний алгоритм, або шифр, — це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем (секретним параметром) — словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифртекст. Ключ забезпечує конфіденційність шифротексту.

Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.

Дешифрування (розкриття шифру) – процес одержання інформації із шифротексту без знання застосованого ключа.

Захищеність шифртекста цілком залежить від двох речей: стійкості криптоалгоритму і таємності ключа.

Стійкість (криптостійкість) - здатність шифру протистояти будь-яким атакам на нього (спробам розшифрувати перехоплене повідомлення, розкрити ключ шифру або порушити цілісність, достовірність інформації.

Стійкість конкретного шифру оцінюється тільки шляхом усіляких спроб його розкриття і залежить від кваліфікації криптоаналітиків, що атакують шифр.

Криптоалгоритм плюс усілякі ключі і протоколи, що приводять їх у дію, складають криптосистему. PGP — це криптосистема.

Криптологія – наука, що складається із двох галузей: криптографії і криптоаналізу.

Криптографія – наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.

Криптоаналіз – наука (і практика її застосування) про методи і способи розкриття шифрів.

Співвідношення криптографії й криптоаналізу очевидне: криптографія – це захист, тобто розробка шифрів, а криптоаналіз – це напад, тобто атака на шифри. Однак ці дві дисципліни пов'язані між собою – не буває гарних криптографів, що не володіють методами криптоаналізу.

«У світі розрізняють два типи криптографії: криптографія, що перешкодить вашій молодшій сестрі читати ваші файли, і криптографія, що перешкодить читати ваші файли урядам великих країн. Ми будемо розглядати криптографію другого типу.»

Криптографія може бути стійкою, а може бути і слабкою, як описано в приведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифртекста відновити вихідний відкритий текст.

Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення.

На практиці для шифрування інформації використовують *методи симетричного і асиметричного шифрування.*

Метод симетричного шифрування передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних.

В асиметричній криптографії для зашифровування даних використовується один ключ, а для розшифровування — інший ключ (звідси і назва — асиметричні). Чим більший ключ (число), тим найбільш захищений отриманий шифртекст.

Переглянути відео «Як працює шифрування?» (про симетричне і асиметричне шифрування) https://www.youtube.com/watch?v=89JyxcVn0lE

Отже, криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований

файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

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. Виконайте інтерактивну вправу «Сучасні методи захисту інформації» **https://learningapps.org/2897461**

Завдання 2. Дослідіть, що таке шифр Цезаря, зашифруйте деякий текст та передайте сусіду праворуч для розшифрування.

Домашнє завдання

1) Опрацювати **конспект**
2) Перегляд відео про історію криптографію «Еволюція криптографії» https://www.youtube.com/watch?v=M9W4QpqQ5Ps
3) **Підготувати** повідомлення про шифрувальну машину Енігма, шифрування RSA.
4) **Дослідити** , як криптографія застосовується у крипто валюті.