МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Завдання і методичні рекомендації для виконання лабораторних робіт для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології, освітній ступінь Бакалавр

ПОЛТАВА – 2021

Завдання та методичні рекомендації для виконання лабораторних робіт із дисципліни «Безпека інформаційних систем» для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології СВО «Бакалавр» підготувала Лариса Дегтярьова. Полтава: ПДАУ, 2021. 44 с.

Укладач: к.т.н., доцент, доцент кафедри Дегтярьова Л.

Рецензент: д.т.н., доцент кафедри Інформаційних систем та технологій Юрій Поночовний

Методичні рекомендації обговорені на засіданні кафедри Інформаційних систем та технологій
Протокол від __ _____ 2021 року № _

Схвалено науково-методичною радою спеціальності
Інформаційні системи та технології
Протокол від __ _____ 2021 року № _

Голова _____ О. Копішинська

ЗМІСТ

ВСТУП

Мета навчальної дисципліни «Безпека інформаційних систем» розкриття сучасних методів захисту інформації в інформаційних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

Основними завданнями вивчення дисципліни «Безпека інформаційних систем» є формування у майбутніх фахівців знань, навичок і умінь, що забезпечують реалізацію захисту конфіденційності інформації; здійснення захисту цілісності інформації; сприяння доступності необхідної інформації.

Компетентності:

Загальні:

- КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.
- КЗ 2. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 3. Здатність до розуміння предметної області та професійної діяльності.

Спеціальні (фахові):

- КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп'ютерно-інтегрованих систем та системної мережної структури, управління ними.
- КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.
- КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Програмні результати навчання:

- ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.
- ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.
- ПР 6. **Демонструвати** знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання

прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

Методи навчання:

усні та методи стимулювання і мотивації: роз’яснення мети вивчення предмета; висування вимог; заохочення;

словесні: пояснення, лекція, інструктаж;

наочні: демонстрація, ілюстрування;

практичні: лабораторна робота;

за логікою: індуктивний, аналітичний, синтетичний, порівняння;

за мисленням: дослідницький, репродуктивний;

інноваційні методи навчання: мультимедійна презентація; дистанційне навчання;

методи самостійної роботи вдома: самостійна робота без керівництва викладача (усні та письмові домашні завдання, завдання самостійної роботи).

Лабораторна робота № 1

Тема: Робота з обліковими записами користувачів і груп ОС Windows Server. Встановлення правил доступу до об’єктів файлової системи

***Мета навчальна**:* формування вмінь створення й редагування облікових записів користувачів ОС Windows Server. Навчитися змінювати власників і правила доступу до об’єктів файлової системи для захисту об'єктів (файлів, процесів).

Мета виховна: виховання свідомого ставлення до праці та навчання, розвиток розумових здібностей, високих моральних якостей, самовдосконалення, індивідуальних здібностей.

***Завдання**:*

1. Ознайомитись з необхідністю створення облікових записів користувачів, які мають певні права безпеки.
2. Створити нові облікові записи користувача та редагувати вже створені. Працювати із диспетчером задач, завершувати завдання та процеси, які не відповідають.

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп’ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

Linux та Windows є багатокористувацькими ОС. Користувачі, що займаються загальними задачами, можуть поєднуватися в групи. Кожен користувач обов'язково належить до одній або декільком групам. Усі команди виконуються від імені визначеного користувача, що належить у момент виконання до визначеної групи. В таких системах необхідно забезпечувати захист об'єктів (файлів, процесів), що належать одному користувачеві, від всіх інших.

Група користувачів — це зібрання облікових записів користувачів, які мають однакові права безпеки. Інколи групи користувачів називаються також групами безпеки.

Обліковий запис користувача може входити до кількох груп. Найбільш поширені групи користувачів - це стандартна група користувачів і група адміністраторів; існують й інші. Для позначення облікового запису користувача часто використовується назва групи користувачів, до якої він входить. Наприклад, обліковий запис, який входить до стандартної групи користувачів, називається стандартним обліковим записом. За допомогою облікового запису адміністратора можна створити власні групи користувачів, перемістити облікові записи з однієї групи до іншої, а також додати або видалити облікові записи, які входять до різних груп. Створивши власну групу користувачів, можна визначати, які права їй призначити.

Обліковий запис, як правило, містить відомості, необхідні для ідентифікації користувача при підключенні до системи, інформацію для авторизації і обліку. Це ім'я користувача та пароль (або інше аналогічний засіб автентифікації — наприклад, біометричні характеристики). Пароль або його аналог, як правило, зберігається в зашифрованому або хешованому вигляді (з міркувань безпеки).

Для підвищення надійності можуть бути, поряд з паролем, передбачені альтернативні засоби автентифікації: наприклад, спеціальне секретне питання (або кілька питань) такого змісту, щоб відповідь було відома тільки користувачеві. Такі питання й відповіді також зберігаються в обліковому записі.

Обліковий запис може містити також додаткові анкетні дані користувача (обов'язково чи опціонально): ім'я, прізвище, по батькові, псевдонім, стать, вік, дата народження, адреса e-mail, домашня і робоча адреса, номер домашнього, робочого та стільникового телефону, номер ICQ, ідентифікатор Skype, інші контактні дані систем миттєвого обміну повідомленнями, адреса домашньої сторінки та/або блогу в інтернеті або інтранеті, відомості про хобі, про коло інтересів, про сім'ю, про перенесені хвороби, про політичні уподобання, про партійну приналежність, про культурні уподобання, про вміння спілкуватися іноземними мовами тощо. Конкретні категорії даних, які можуть бути внесені в таку анкету, визначаються творцями і (або) адміністраторами системи.

Обліковий запис може також містити одну або декілька фотографій або аватар користувача.

Обліковий запис користувача також може враховувати різні статистичні характеристики поведінки користувача в системі на основі відстежень системи: давність останнього входу в систему, тривалість останнього перебування в системі, адреса використаного при підключенні комп'ютера, інтенсивність використання системи, сумарне і (або) питома кількість певних операцій, зроблених у системі тощо.

Методи навчання:

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1. Ознайомитись з необхідністю створення облікових записів користувачів, які мають певні права безпеки

1. Для використання комп'ютера під управлінням Windows необхідно спочатку створити обліковий запис користувача, що складається з імені користувача і пароля. Після натиснення CTRL+ALT+DEL (якщо встановлена відповідна опція) і введення імені користувача і пароля у Windows здійснюється їх перевірка. Якщо обліковий запис користувача був вилучений, то у Windows будуть блокуватися будь-які спроби доступу за допомогою даного облікового запису. Для виконання задач на комп'ютері із встановленою ОС Windows користувачі повинні мати певні права. Використання облікових

записів груп користувачів дозволяють швидко і просто призначати користувачам відповідні права і дозволи. В ОС Windows передбачено кілька вбудованих облікових записів груп користувачів, організованих залежно від задач, які часто виконуються користувачами. Включення користувачів до одного чи кількох з вбудованих облікових записів груп дозволяє надати більшій частині користувачів прав, що їм необхідні для розв'язування їх задач. Правами користувача називаються правила, за допомогою яких надають користувачеві перелік дозволених операцій на даному комп'ютері. Крім того, права користувача визначають можливість безпосереднього входу в систему (на локальному комп'ютері) чи до мережі, можливість додавання користувачів в локальні групи, вилучення користувачів і т.п. Вбудовані облікові записи груп включають набір вже призначених прав користувача. Як правило, адміністратори призначають права користувача шляхом додавання облікового запису користувача до одного з вбудованих облікових записів груп або шляхом створення нової групи та призначення їй певних прав користувачів. Користувачам, що будуть приєднані до групи, автоматично надаються всі права користувачів, вказані в обліковому записі групи. Управління правами користувача здійснюється за допомогою групової політики. Доступ до ресурсів мережі глобальних користувачів і груп контролюється адміністратором. Управління доступом користувачів і груп до ресурсів мережі важливі для безпеки ОС Windows, оскільки це дозволяє обмежити можливості користувачів і груп виконувати певні дії шляхом призначення їм прав і дозволів. Перелік прав визначає дозволи користувачеві виконувати на комп'ютері певні дії, такі як архівація файлів і папок, завершення роботи комп'ютера тощо. Дозвіл являє собою правило, пов'язане з об'єктом (наприклад файлом, папкою чи принтером), за яким визначається, яким користувачам і якого типу доступ до об'єкта дозволений. Облікові записи користувачів і груп важливі для забезпечення безпеки комп'ютера та інформаційних ресурсів. Для налаштування облікових записів і груп потрібно скористатися послугою Керування комп'ютером (Панель управління, Адміністрування).

2. В папці *Локальні користувачі та групи* існує 2 папки: *Користувачі* та *Групи*. В папці *Користувачі* відображається два вбудовані облікові записи користувачів – *Адміністратор* і *Гість*, а також всі створені облікові записи користувачів. Наявність цього облікового запису дозволяє виконувати необхідні дії до того, як користувач створить свій власний обліковий запис. Обліковий запис адміністратора є елементом облікового запису групи адміністраторів на робочій станції або сервері.

Створення локального ОЗК (Облікові записи користувачів (User accounts).)

Це можливо в якості адміністратора. Послідовність дій.

1) Пуск (Start) → Панель керування (Control panel) → Облікові записи користувачів (User accounts).

2) У вікні "ОЗК" (User accounts) в розділі "Виберіть завдання" (Pick a task) виберіть "Створення облікового запису" (Create a new account). Windows XP виводить вікно "Введіть ім'я для нового облікового запису" (Name the new account).

3) У текстовому полі "Ввести ім’я для нового облікового запису" (Type a name for the new user) вводимо User1. Натиснути NEXT. Windows XP виводить діалогове вікно "Вибір типу облікового запису" (Pick an account type).

4) Включаємо "Обмежений запис" (limited). Якщо маємо обмежений тип облікового запису то можна:

• змінити або видалити свій пароль;

• змінити зображення власного облікового запису, тему, параметри робочого столу; • проглянути створені файли;

• переглянути файли, що використовуються разом.

5) Натискаємо кнопку "Створити обліковий запис" (Create account). Windows XP виводить вікно "Облікові записи користувачів"

6) Створюємо другий обліковий запис (User2). Для цього повторюємо пункти 3-6.

Вікно "ОЗК" (User accounts) не зачиняємо. Воно знадобиться пізніше.

Призначення пароля локальному обліковому запису користувача

Послідовність дій.

1) У вікні "ОЗК" (User accounts) вибираємо User1.

2) Вибираємо "Створити пароль" (Create password).

3) Розмістіть "password" в полі "Введіть пароль" (Type new password) та в полі "Введіть пароль для підтвердження (Type the new password again to confirm).

4) Введіть слово або фразу, яка є підказкою про пароль (Type a word or phrase to use as a password hint).

5) Натисніть "Створити пароль" (Create password).

6) З’являється вікно "Що ви бажаєте змінити в ОЗК User1? (What do you want to change about User1?) Список можливих змін "включає два варіанти":

• "зміна пароля" (Change the password);

• "Видалення пароля" (Remove the password).

7) Для повернення у вікно "ОЗК" (User accounts) виділіть знак "Додому" (Home).

8) Для облікового запису User2 призначте пароль User2. 27

9) Закрийте вікно "ОЗК" (User accounts) та панель керування.

Видалення локального ОЗК

Зробіть це на прикладі користувача User2. Ця процедура виконується адміністратором.

1) На панелі керування виділіть "ОЗК" (User accounts).

2) Виділіть User2. Windows XP виведе вікно "Що ви бажаєте змінити в ОЗК User2? (What do you want to change about User2 account?).

3) Виділіть "Видалення облікового запису" (Delete the account). Windows XP виведе вікно "Бажаєте зберегти файли, які належать User2? (Do you want to keep User2 files?).

4) Виберіть "Видалити файли" (Delete files). Windows XP виведе вікно "ОЗК" (User accounts). ОЗК User2 на сторінці "Виберіть ОЗ, що змінюється" (Or pick an account to change) відсутня.

5) Закрийте категорію "ОЗК" (User accounts) та панель керування.

6) Кінець.

Отже,

1. Категорія "ОЗК" (User accounts) дозволяє адміністратору: створювати новий ОЗК; змінювати існуючий ОЗК, спосіб входу в систему або завершення сеансу.

2. Прапорці, що призначені для зміни способу входу в систему "Використати сторінку привітання" (Use the welcome screen) або завершення сеансу "Швидка зміна користувачів" (Use fast User switching), використовуються для усіх користувачів.

3. Завжди вимагайте, щоб користувачі змінювали свої паролі при кожному вході в систему.

4. При використанні сторінки привітання та швидкої зміни користувачів після завершення сеансу з’являється вікно діалогу, що дозволяє переключатись на інший обліковий запис без попереднього завершення сеансу та закриття запущених програм.

Завдання 2: Створювати нові облікові записи користувача та редагувати вже створені. Працювати із диспетчером задач, завершувати завдання та процеси, які не відповідають

1. Вивчити засіб налаштування аутентифікації, реалізованої при вході в операційну систему Windows. Для цього необхідно запустити утиліту «Облікові записи користувачів», набравши в командному рядку ім'я утиліти control userpasswords2 або з меню «Мій комп'ютер/керування/локальні користувачі й групи». Зробити зміни залежно від варіанта.

2. Налаштувати доступ користувачів і груп до файлів і директорій операційної системи Windows, для цього відкрити властивості директорії й вибрати вкладку «Безпеки» «Security». Зробити зміни, залежно від варіанта.

3. Настроїти розмежування прав доступу користувачів і груп до ОС Windows за допомогою настроювання локальної політики, для цього запустити з командного рядка утиліту secpol.msc. Зробити зміни залежно від варіанта.

4. Налаштувати необхідні служби для роботи локального комп'ютера, відповідно до варіанта, для цього запустити утиліту services.msc.

5. Ознайомитися з настроюванням забезпечення безпеки ОС Windows, за допомогою оснащення «Налаштування системи», для цього запустити з командного рядка утиліту msconfig. Зробити зміни залежно від варіанта.

6. Налаштувати файл завантаження системи. Для цього необхідно, залежно від варіанта, зробити зміни параметрів завантаження у файлі C:\boot.ini.

7. Настроїти рівні доступу в Інтернет стандартними способами ОС Windows Internet Explorer (низький, середній, високий). Зробити зміни, залежно від варіанта.

8. Настроїти засоби автоматичного відновлення ОС Windows. Зробити зміни залежно від варіанта.

9. Настроїти стандартний брандмауер ОС Windows (рівень захищеності – низький, середній, високий). Зробити зміни залежно від варіанта.

10. Забезпечити захист даних локальної робочої станції, за допомогою

реєстру, для цього запустити утиліту RegEdit і зробити зміни залежно від варіанта.

Порядок і рекомендації щодо виконання роботи

1. Надати інформацію про виконання ОС з власними параметрами щодо налаштування облікових записів користувачів і груп ОС Windows Server з використанням покрокової демонстрації скріншотами, які супроводжуються текстовими поясненнями, виконати індивідуальне завдання.
2. У ході виконання лабораторної роботи, необхідно включити змінені параметри, інструмент (утиліти, команди), за допомогою яких вироблялися зміни, опис призначення кожного зміненого параметра й зроблених вами налаштувань.
3. Дати відповідь на контрольні питання:

   1). Які бувають типи облікових записів користувачів?

   2). На якому ПК локальні облікові записи дозволяють вхід в систему та доступ до ресурсів?

   3). Можливо чи ні змінити тип облікового запису користувача?

   4). Як налагодити облікові записи користувачів для безпечної роботи?

   5). Чому не слід працювати на комп'ютері, використовуючи обліковий запис адміністратора?

   6). Як перемкнутися на інший обліковий запис користувача?

   7). Яка максимальна кількість символів при створенні імені ОЗК?

   8). Які символи неприпустимі при створенні імені ОЗК?

   9). Яка кількість символів при створенні пароля ОЗК?

   10). Яке призначення паспорту .NET?
4. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

   – № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

   – результати виконання завдань № 1,2;

   – відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.

3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_01_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп’ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.

2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.

3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.
4. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Лабораторна робота 2

Тема: Використання теорії чисел для захисту інформації.

Мета навчальна: розглянути базові поняття теорії чисел, отримання практичних навичок шифрування і дешифрування повідомлень за допомогою відкритого та закритого ключа криптосистеми RSA з використанням теорії чисел.

Мета виховна: виховувати зібраність, самовладання, комунікативність.

Завдання:

1. Розглянути приклади застосування теорії чисел в криптографії.
2. Виконати розрахунок ключів криптосистеми RSA за власними варіантами.

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

Під ключем в криптографії розуміють змінний елемент шифру, який застосовують для шифрування конкретних повідомлень.

Шифрування — процес вживання шифру і інформації, що захищається, тобто перетворення інформації, що захищається, в шифроване повідомлення за допомогою певних правил, що містяться в шифрі.

Шифр — спосіб (метод), перетворення інформації з метою її захисту від незаконних користувачів.

В асиметричних алгоритмах шифрування (або криптографії з відкритим ключем) для зашифровування інформації використовують один ключ (відкритий), а для розшифрування - інший (секретний). Ці ключі різні і не можуть бути отримані один з іншого.

У асиметричному шифруванні використовується два пароля - один відкритий (публічний) і один закритий (секретний). Відкритий пароль відсилається всім людям, закритий же пароль залишається на стороні сервера або іншого приймача. При цьому назви часто умовні, так як зашифроване повідомлення одним з ключів можна розшифрувати тільки за допомогою іншого ключа. Іншими словами, ключі в цьому сенсі рівноцінні.

Такі алгоритми шифрування дозволяють вільно поширювати пароль (ключ) по мережі, так як без другого ключа неможливо отримати вихідне повідомлення. Надійність шифрування (криптографічний стійкість) залежить від довжини ключа і експоненціально зростає при збільшенні довжини ключа в два рази.

Асиметричне шифрування застосовується в різних протоколах таких, як SSH і SSL/TLS, а також в різних системах, що вимагають установки безпечного з'єднання в незахищеній мережі або перевірки цифрового підпису.

В даний час використовуються наступні алгоритми асиметричного шифрування:

- RSA алгоритми можна використовувати як для шифрування, так і для створення цифрової (електронної) підписи. RSA знаходить застосування в різних середовищах, в тому числі, і при створенні захищеного каналу зв'язку за технологією SSL (Secure Sockets Layer). Важливо відзначити, що симетричний ключ нікуди не передається, оскільки у кожного з партнерів він виробляється безпосередньо «на місці».

- Diffie-Hellmann обмін ключами (Diffie-Helmann key exchange) має ім'я відповідно до іменами його творців. Вважається, що саме вони заснували методологію пари відкритого і закритого ключів. Його використовують в основному для безпечного пересилання ключів через глобальні мережі.

- Криптосистема еліптичних кривих (ECC - Elliptic Curve Cryptography) посвоєму функціонуванню подібна до RSA алгоритмом. Її застосовують в основному в малих системах (таких як мобільні телефони і бездротові пристрої).

В основу криптостойкости RSA покладена задача факторизації (розкладання на множники) великих (понад 200 двійкових розрядів) цілих чисел. Найбільш поширеним асиметричним алгоритмом шифрування є RSA, який використовується в протоколі SSL / TLS і застосовуваний як для шифрування, так і для цифрового підпису.

Процедури генерації ключів, шифрування і дешифрування для цього алгоритму представлені на рис. 2.1.

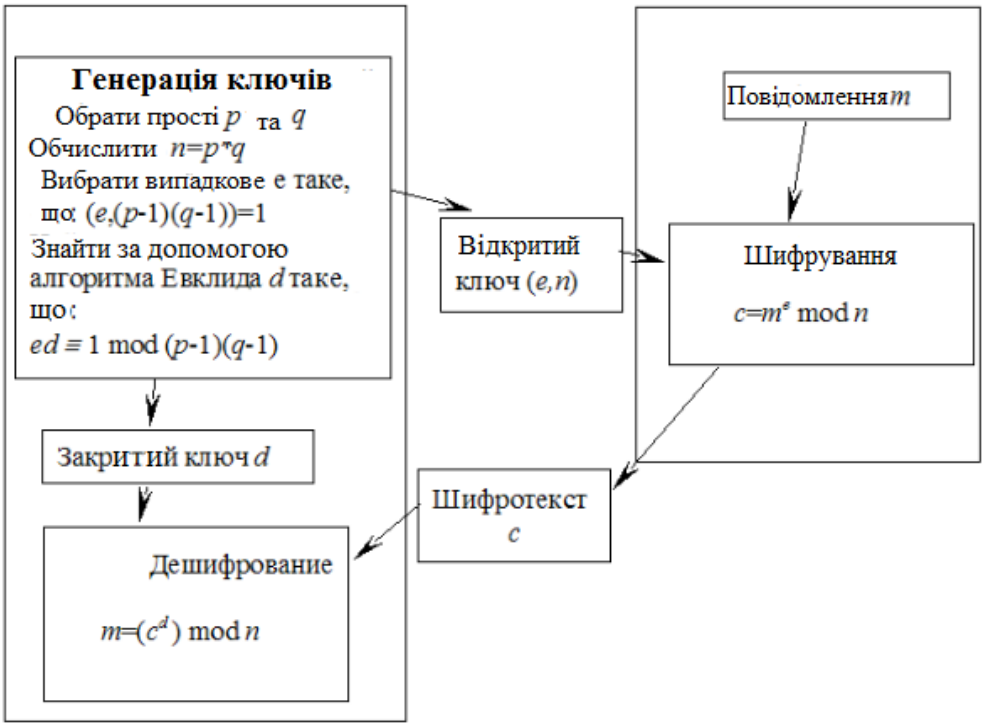

Рис. 2.1 Процедури генерації ключів, шифрування і дешифрування для алгоритму RSA

В основі алгоритму лежить обчислювальна складність завдання факторизації великих цілих чисел. Довжина ключа RSA зазвичай становить 1024 або 2048 біт. Однак деякі організації переходять на 2048-бітові ключі.

Основні поняття теорії чисел

Визначення 1. Говорять, що *a* ділиться на *b*, якщо $a = bq$ і $q \in z$. При цьому *a* називають кратним числа *b*, а *b*- дільником числа *a*.

Теорема 1 (про розподіл із залишком). Будь-яке ціле *a* можна представити за допомогою позитивного цілого числа *b* рівністю виду a= bq + r, $0 \le r < b$. Число *q* називається неповним приватним, а число *r*-остатком від розподілу *a* на *b*.

Визначення 2. Будь-яке ціле, яке ділить одночасно цілі *a*, *b* називаються їх загальним дільником.

Визначення 3. Найбільший із загальних дільників чисел *a* і *b* називається загальним найбільшим дільником і позначається символом (a,b). Якщо (a,b)=1 то цілі *a* і *b* називають взаємно простими.

Теорема 2. Якщо $a = bq + c,$ то (a, *b*) =(*b, c*).

Для пошуку (a, *b*), при $a > b$ застосовується алгоритм Евкліда, що базується на теоремі 2.

2. Алгоритм Евкліда

Для того, щоб число d було найбільшим загальним дільником чисел $a_1 ... a_n$ повинні виконуватися наступні три умови:

1) $d <$);

2) $d|a_1,...,d|a_2$;

3) Якщо, то $\delta_{,}\imath_1,...,\delta_{,}\imath_2$, то $\delta_{,}l$;

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1. Розглянути приклади застосування теорії чисел в криптографії.

Приклад 1. Визначити, чи є пара ключів (*n*, *e*) = (3403, 137), (*n*, *d*) = (3403,2873) ключами криптосистеми RSA, якщо $n = pq$, де p , q - прості числа:

$p = 41$, $q = 83$.

Рішення

Якщо дана пара ключів є ключами криптосистеми RSA, то вона повинна задовольняти наступному співвідношенню: $ed \equiv 1(\mathrm{mod}\varphi(n))$.

$$ed = 2873 \cdot 137 = 393601$$

$$\varphi(3403) = (p-1)(q-1) = (41-1)(83-1) = 40 \cdot 82 = 3280$$

$$ed = 393601 \equiv 1(\mathrm{mod}\ 3280)\ .$$

Дана пара ключів задовольняє співвідношенню, значить вона є ключами RSA.

Приклад 2. Знайти значення виразу: $2302^{2873} \pmod{3403}$.

Рішення

e = 2873 =101100111001

1) 2302
2) $2301^2 \pmod{3403} = 733$
3) $733^2 \pmod{3403} = 3018$
4) $3018^2 \pmod{3403} = 1896$
5) $1896^2 \pmod{3403} = 1248$
6) $1248^2 \pmod{3403} = 2333$
7) $2333^2 \pmod{3403} = 1492$
8) $1492^2 \pmod{3403} = 502$
9) $502^2 \pmod{3403} = 182$
10) $182^2 \pmod{3403} = 2497$
11) $2497^2 \pmod{3403} = 713$
12) $713^2 \pmod{3403} = 1322$

$$2302 \cdot 1896 \cdot 1248 \cdot 2333 \cdot 182 \cdot 2497 \cdot 1322 (\mathrm{mod} 3403)$$

1946

2269

1912

878

834

3379

$2302^{2873} \pmod{3403} = 3379$.

Завдання 2. Виконати розрахунок ключів криптосистеми RSA за власними варіантами.

1. Визначити які пари ключів (n,e), (n,d) є ключами криптосистеми RSA, якщо $n=pq$, де, p, q - прості числа.

Варіанти завдань

Варіант	p , q - прості числа	Пара ключів (n, e) (n, d)
1	$p = 43,\ 103$	(4429, 170) (4429, 15724)
2	$p = 47,\ 107$	(5029, 26962) (5029, 163)
3	$p = 53,\ 109$	(5777, 629) (5777, 125)
4	$p = 59,\ 113$	(6667, 2995) (6667, 161)
5	$p = 61,\ 127$	(7747, 4827) (7747, 142)
6	$p = 67,\ 131$	(8777, 1283) (8777, 107)
7	$p = 71,\ 137$	(9727, 12382) (9727, 102)
8	$p = 73,\ 139$	(10147, 19718) (10147, 116)
9	$p = 79,\ 149$	(11771, 293) (11771, 197)

10	$p = 83,\ 151$	(12533, 1869) (12533, 138)

2. Знайти значення виразу:

Варіант	
1	$4827^{5436} (\text{mod } 32391)$
2	$3902^{5447} (\text{mod } 21726)$
3	$1869^{9894} (\text{mod } 28703)$
4	$4664^{7711} (\text{mod } 28253)$
5	$6868^{8723} (\text{mod } 9741)$
6	$3035^{1842} (\text{mod } 30106)$
7	$9040^{8942} (\text{mod } 19264)$
8	$6729^{3548} (\text{mod } 19629)$
9	$4966^{7376} (\text{mod } 13931)$
10	$5537^{2082} (\text{mod } 22929)$

Порядок і рекомендації щодо виконання роботи

1. Вивчити теоретичні відомості по теорії чисел в криптографії.
2. Виконати розрахунки за власним варіантом. Результати розрахунків продемонструвати з покроковим виконанням.
3. Дати відповідь на контрольні питання:
4. Яка довжина ключа RSA?
5. З яких дій складається процедура генерації ключів?
6. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

– відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.

3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_02_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.

2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.

Лабораторна робота № 3

Тема: Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіка

Мета навчальна: Виявлення вторгнень у мережі Windows, виявлення сканування портів, повідомлення про спроби вторгнень. Вивчити на практиці механізм захисту локальних мереж за допомогою моніторингу. Для цього вивчити основи роботи з утилітами моніторингу мережного трафіка в локальній мережі, на прикладі Network Monitor

Мета виховна: виховати інформаційну культуру, уміння працювати в групі, формування позитивного ставлення до навчання

Завдання

1. Ознайомитись з призначенням та характеристиками утиліти Network Monitor. Порівняти її функції з функціями утиліти Iris The Network Traffic Analyzer.

2. Виконати налаштування Network Monitor для забезпечення організація безпеки локальної мережі.

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

Network Monitor поставляється у двох версіях: спрощеній, котра включена в ОС Windows і повній, що ввійшла до складу окремого продукту Systems Management Server. Спрощена версія може контролювати тільки локальний трафік, тобто тільки ті кадри, які приймаються мережним адаптером робочої станції, що відслідковується.

Повна версія програми фіксує повністю весь трафік у мережі, при підключенні до іншого сервера або робочої станції, на яких установлений Network Monitor і дозволяє контролювати вилучену систему.

В утиліту Network Monitor входять фільтри, що дозволяють виділити спеціальну інформацію при більших мережних потоках; фільтри захвата, що вибирають із всієї захопленої інформації ту, котра необхідна; і тригери, що дозволяють системі виконувати певні дії з даними, що утримуються в пакетах.

Після запуску програми, вибирається мережа, трафік якої буде контролюватися.

Вибір мережі робиться за допомогою меню Capture і пункту Networks. У панелі, що з'явилася, відображаються всі мережні інтерфейси, які є в даному

комп'ютері, мережні адаптери, COM-порти служби RAS, якщо вона встановлена на комп'ютері.

Утиліта Iris The Network Traffic Analyzer, крім стандартних функцій збору, фільтрації й пошуку пакетів, побудови звітів, має можливість реконструювання даних. Iris The Network Traffic Analyzer допомагає відтворити сеанси роботи користувачів з різними ресурсами.

Технологія реконструювання даних, реалізована в модулі дешифрування (decode module), яка перетворює зібрані двійкові мережні пакети у вихідний вид, розширюючи можливості наявних засобів моніторингу й аудита.

Аналізатор пакетів, дозволяє зафіксувати різні деталі атаки, такі як дата й час, IP-адреси й DNS-імена комп'ютерів зловмисника, а також використані порти.

Аналізатор пакетів, може відтворити точну, аж до натискання клавіш і рухів миші, картину вторгнення, що необхідна для усунення наслідків атаки й посилення заходів безпеки. Аналізатор пакетів дозволить підсилити захист корпоративної мережі.

Утиліта Network Monitor використовується для аналізу й виявлення проблем у мережі. Network Monitor записує дані, передані й отримані комп'ютерами мережі, для наступного перегляду й аналізу цих даних. Кадри й пакети канального рівня записуються через прикладний рівень і представляються в графічному виді. Кадри й пакети містять інформацію:

– адресу відправника й адресата;

– порядкові номери;

– контрольні суми.

Утиліта Network Monitor розшифровує цю інформацію, дозволяючи аналізувати мережний трафік і вести журнал мережної активності. Крім даних канального рівня, Network Monitor відображає деякі дані прикладного рівня, наприклад протоколи http або FTP.

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1. Ознайомитись з призначенням та характеристиками утиліти Network Monitor. Порівняти її функції з функціями утиліти Iris The Network Traffic Analyzer.

1. Запустіть утиліту Network Monitor. Ознайомтеся з основними механізмами моніторингу мережного трафіка, а також з настроюваннями, представленими в пунктах меню Вид (View), Фрейми (Frames), (Capture), Фільтр (Filter), Властивості (Tools).

2. Настройте й запустіть перехоплення трафіка, залежно від вашого варіанта. Для цього скористайтеся вікном редактора фільтра запису (Capture Filter) або фільтра перегляду (Display Filter), що відкривається з вікном Capture.

Через деякий час зупиніть перехоплення заданого трафіка. Для цього у меню Capture виберіть меню зупинки перехоплення.

3. Проаналізуйте отриманий мережний трафік. Занесіть до протоколу правило фільтра, яке ви використовували.

4. Запустіть утиліту eEye Iris. Ознайомтеся з основними механізмами моніторингу трафіка, а також з настроюваннями, представленими в основних пунктах меню.

5. Запустіть сканування трафіка. Через деякий час зупиніть утиліту. Виберіть фільтри перегляду, залежно від завдання.

7. Порівняйте роботу двох, вивчених вами в даній лабораторній роботі, утиліт. Опишіть у протоколі розходження, достоїнства й недоліки кожної з них.

Завдання 2. Виконати налаштування Network Monitor для забезпечення організація безпеки локальної мережі

Варіанти завдань для виконання лабораторної роботи
(Налаштування параметрів фільтрів):

1. Налаштуйте перехоплення трафіка між двома сусідніми робочими станціями.

2. Налаштуйте перехоплення трафіка між локальною робочою станцією й сусідньою.

3. Налаштуйте перехоплення за протоколом ARP.

4. Налаштуйте запис кадрів, що містять певний тип даних.

5. Налаштуйте перехоплення всього мережного трафіка.

6. Налаштуйте перехоплення тільки зовнішнього трафіка.

7. Відфільтруйте кадри для відображення широкомовних пакетів у мережі.

8. Відфільтруйте кадри для відображення адреси відправника й приймача кадру для канального й мережного рівнів.

9. Відфільтруйте кадри щоб відобразити кадри, для відправлення яких використовувався протокол ftp.

10. Відфільтруйте кадри щоб відобразити кадри, передані за протоколом TCP.

11. Відфільтруйте кадри щоб відобразити кадри, передані за протоколом IP

12. Відфільтруйте кадри щоб відобразити весь мережний трафік, крім широкомовних повідомлень.

Порядок і рекомендації щодо виконання роботи

1. Розберіть рядок записаних даних і структуру кадрів у кожній з утиліт.
2. Ознайомтеся з типами фільтра відображення й занесіть до звіту таблицю різних способів фільтрування.
3. Дати відповідь на контрольні питання:
    a. На якому рівні семирівневої моделі OSI виробляється збір даних в утиліті Network Monitor?
    b. Для чого потрібна утиліта Microsoft Network Monitor?
    c. Яку інформацію про передані й отримані дані за мережею бачить адміністратор за допомогою утиліти Network Monitor?

d. Для чого служить і яким чином настроюється фільтр запису утиліти Network Monitor?
e. Для чого служить і яким чином настроюється фільтр відображення утиліти Network Monitor?
f. Яким чином можливе виявлення утиліти Network Monitor і яка інформація видається при виявленні даної утиліти?
g. Для чого потрібна утиліта eEye Iris?
h. Які настроювання й фільтри можна застосовувати в утиліті eEye Iris?
i. Дайте порівняльну характеристику Network Monitor і eEye Iris?
j. Поясніть, яким чином можна одержати інформацію про зловмисника за допомогою утиліт Network Monitor і eEye Iris?

4. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

До звіту з ЛР внесіть відомості за обраного сегменту мережі, залежно від вашого завдання. Відомості повинні містити інформацію:

– про використання мережі;

– про кількість отриманих байт у секунду;

– про кількість отриманих кадрів у секунду.

Відомості повинні включати наступну інформацію:

– статистику сеансу;

– статистику робочої станції;

– загальну статистику;

– відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.

3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_03_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.

2. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.

3. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Лабораторна робота № 4

Тема: Організація безпеки механізму аутентифікації при перехопленні парольних хешей і їхньої розшифровки

Мета навчальна: вивчення на практиці, основ роботи з утилітами перехоплення й розшифровки парольних хешей програмою *Cain&Abel* (*ПЗ у вільному доступі*), при аутентифікації за мережею, для перевірки коректної роботи механізму аутентифікації

Мета виховна: умотивувати необхідність знань про конфіденційність та умови доступу до особистих даних, сприяти розвитку компетентності в галузі використання інформаційно-комунікаційних технологій.

Завдання

1. Ознайомлення з призначенням, можливостями й принципом роботи утиліти Cain&Abel (безкоштовної версії ПЗ) - інструменту відновлення паролів для операційних систем Windows, який може захищати від вразливостей в механізмі кешу, методах аутентифікації і стандартах мереженого протоколу
2. Здійснити перебір паролів методом, залежно від варіанта

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

Автентифіка́ція — процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Один із способів автентифікації в інформаційній системі полягає у попередній ідентифікації на основі користувацького ідентифікатора і пароля — певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом в мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі значенням, яке зберігається в спеціальній захищеній базі даних і, у випадку успішної автентифікації проводить авторизацію з подальшим допуском користувача до роботи в системі.

Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційної системи. Під несанкціонованим доступом до інформації розумітимемо доступ до інформації, що порушує встановлені правила розмежування доступу і здійснюваний з використанням штатних засобів обчислювальної техніки або автоматизованих систем. НСД може носити випадковий або навмисний характер. Задачею систем ідентифікації і аутентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи.

Основне завдання утиліти Cain&Abel це відновлення паролів. Відновити можна паролі входу в систему, загальні паролі, паролі екранної заставки, паролі доступу до мережі й будь-які інші, кэшируємі в системі, у зовнішньому PWL-Файлі або в системному реєстрі. Cain&Abel не використовує системних уразливостей, однак має досить потужні засоби дешифрування.

Програма Cain&Abel за принципом дії не ставиться до мережних сканерів, але демонструє одну з методик зловмисників, використовувану для збору інформації про атакуєму систему. У результаті успішно проведеної операції, названої розроблювачами Arp Poison Routing (APR), на обрані комп'ютери впроводжують сфальсифіковані зв'язки мережних і апаратних адрес комп'ютерних систем. У результаті весь трафік між атакованими комп'ютерами починає пересилатися через систему зловмисника. Утиліта Cain&Abel дозволяє виступати одночасно в якості ARP spoofer і перехоплювача RDP трафіка між обраними вузлами.

Cain and Abel дозволяє відновлювати загублені паролі для операційних систем сімейства Windows. Підтримується декілька режимів відновлення: грубий злом методом перебору, підбір за словником, перегляд прихованих зірочками паролів і т.д. Також присутні опції для виявлення пароля шляхом перехоплення інформаційних пакетів та їх подальшого аналізу, записи переговорів по мережі, аналізу кеша і ін.

Крім того, програма здатна визначати паролі, приховані "зірочками", а також включає в себе аналізатор мережевих протоколів.

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1: Ознайомлення з призначенням, можливостями й принципом роботи утиліти Cain&Abel - інструменту відновлення паролів для операційних систем Windows, який може захищати від вразливостей в механізмі кешу, методах аутентифікації і стандартах мереженого протоколу

1. Необхідно запустити програму. Ознайомтесь з можливостями основних пунктів меню: Конфігурації (Configure), Сервіс (Tools).

2. Створіть на вашій робочій станції кілька локальних користувачів з паролями різної довжини й складності. При створенні користувачів не встановлюйте флаг «User must change password at next logon». Також створіть загальний каталог, з ім'ям «Test», і надайте створеним вами користувачам права на нього.

3. Відкрийте пункт меню Конфігурації (Configure), на вкладці «Sniffer», виберіть ваш мережний адаптер і натисніть OK. Потім натисніть на кнопку Start Sniffer і перейдіть на вкладку Sniffer, у ній на вкладку Passwords, для того щоб переглянути інформацію про перехоплені паролі.

4. Попросіть сусіда підключитися до вашого комп'ютера за мережею від

імені створених вами користувачів, для цього можна скористатися меню директорії «Сервіс» (Service), «Підключити мережний диск» (Map Network Drive) із параметром «Підключити, використовуючи ім'я» (Connect using a different user name). Переконайтеся, що в контейнері SMB є перехоплені парольні хеші.

5. Переглянете кількість завантажених хеш. Для цього в контекстному меню Send all to Cracker виберіть перехоплені парольні хеші, із вкладки Cracker, потім виберіть меню (Dictionary Attack NTLM + Challenge) для перегляду інформації про кількість завантажених хеш.

6. Здійсніть перебір паролів методом, залежно від вашого варіанта.

7. Протестуйте пароль, за допомогою команди «Тестувати пароль» (Test Password), контекстного меню.

8. Після закінчення лабораторної роботи видаліть створених вами користувачів і мережних дисків.

Завадання 2: Здійснити перебір паролів методом, залежно від варіанта

Варіанти завдань для виконання Завдання 2 лабораторної роботи №4 (Метод перебору):

1. Здійсніть перебір паролів за словником. Для цього у вікні «Словник» (Dictionary Crack) виберіть пункт «Додати» (Add) і виберіть файл Wordlists.txt у директорії Wordlists, поверніться до меню «Словник» (Dictionary Crack) і виберіть пункт «Почати» (Start), для перегляду як відбувається перебір паролів за словником.

2. Здійсніть перебір паролів «грубою силою». Для цього, скористайтеся пунктом контекстного меню «Атака» (Brute-Force Attack NTLM + Challenge). Подивіться, як оцінить необхідний час для перебору утиліта Cain. При великих часових витратах виберіть пароль з меншою довжиною. На основі проробленої роботи, занесіть до протоколу вимоги, які, на вашу думку, необхідно пред'являти до пароля.

3. Проскануйте MAC-адреси робочих станцій у вашій локальній мережі. Для цього відкрийте вкладку «Sniffer», перейдіть у режим сніфінгу, виберіть «Star/Stop Sniffer» і додайте «SCAN MAC addresses». Після виявлення робочих станцій у локальній мережі, на вкладці «Sniffer», перейдіть на вкладку «ARP».

Додайте правила ARP Poison routing для того, щоб ваша робоча станція виступала в ролі сніфера між обраними сусідніми робочими станціями з лівих і правих полів. Не виключаючи режим сніфера, виберіть меню «Start/Stop ARP» для того, щоб відслідковувати обмін пакетами й поступово наповнювати рядки Passwords, поки не зміниться поле ARP-RDP на (1).

4. Використовуйте для перехоплення пароля меню Конфігурації (Configure), «Фільтр і перемикання портів» (Filters and Ports Tab), щоб захоплювати тільки аутентифікаційну інформацію. Здійсніть відновлення пароля за допомогою перегляду схованих паролів.

5. Використовуйте для перехоплення пароля меню HTTP Fields Tab, що містить список імені і поля пароля.

6. Здійсніть перебір паролів за допомогою методу Cryptanalysis.

7. Здійсніть перебір паролів за допомогою методу Brute-Force.

8. Здійсніть перебір паролів за допомогою виявлення пароля шляхом перехоплення інформаційних пакетів і їх наступний аналіз кеш.

9. Здійсніть перебір паролів за допомогою виявлення пароля шляхом перехоплення інформаційних пакетів і їх наступний аналіз запису переговорів за мережею.

10. Здійсніть перебір паролів за допомогою «атаки за маскою».

11. Здійсніть перебір паролів за допомогою «гібридної атаки».

12. Здійсніть перебір паролів за допомогою «атаки розподіленим перебором».

Порядок і рекомендації щодо виконання роботи

1. У звіті до лабораторної роботи опишіть методи, які застосовуються для відновлення пароля в утиліті Cain&Abel, а також опишіть, яким чином реалізуються ці можливості. Докладно опишіть метод, яким ви скористалися.

2. Розробіть план використання механізмів запобігання злому пароля схожими утилітами. Опишіть всі існуючі можливості запобігання злому пароля із внутрішньої мережі та із глобальної мережі Інтернет.

3. Дайте відповідь на контрольні питання:

   a. Опишіть призначення, можливості й принцип роботи утиліти *Cain&Abel.*

   b. Поясніть, для чого потрібний протокол ARP і опишіть принцип здійснення атаки з його використанням?

   c. Для чого необхідне виконання ARP-spoofing в утиліті *Cain&Abel?*

   d. Які вимоги до пароля, як адміністратор безпеки, ви б пред'являли у вашій локальній мережі?

   e. Якими методами, можна, відновити пароль за допомогою утиліти *Cain&Abel?*

   f. Опишіть, як відбувається відновлення пароля за словником?

4. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

– відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.

3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_04_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.
2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.
4. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Лабораторна робота № 5

Тема: Налаштовування та адміністрування міжмережних екранів (4 години)

Мета навчальна: вивчення структури, функцій та набуття навичок налагодження та технічної експлуатації міжмережних екранів (брандмауерів), реалізованих у локальних обчислювальних мережах (ЛОМ) та автоматизованих робочих місцях (АРМ).

Мета виховна: виховання свідомого ставлення до праці та навчання, розвиток розумових здібностей, високих моральних якостей, самовдосконалення, індивідуальних здібностей.

Завдання

1. Ознайомитись з типами політик мережного доступу, технічної реалізації цих політик, вибір типів міжмережних екранів для забезпечення безпеки ЛОМ, порядок їх реалізації і технічної експлуатації.
2. Знайомство з комплексом засобів міжмережного екрану Agnitum Outpost Firewall (програмної та апаратної частин), встановленого на ОС MS WINDOWS.

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

Міжмережевим екраном (МЕ) (брандмауер\firewall) називають локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить до інформаційної системи і/або виходить з інформаційної системи.

МЕ служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, вспливаючі вікна та інше, не надсилати «чужим» серверам інформацію про комп'ютер користувача ІС.

Функціонування брандмауеру полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує. Ефективність роботи брандмауера, що працює під управлінням Windows, зумовлена тим, що він повністю заміщує реалізований стек протоколів TCP\IP, і тому порушення його роботи хакерами з допомогою спотворення протоколів зовнішньої мережі є неможливим.

Архітектурно Internet-системи являють собою трирівневі системи "клієнт-сервер" з використанням WWW-сервера в якості ПО як проміжного шару. Оскільки саме трирівневі системи звичайно використовуються для найбільш ефективної роботи механізмів безпеки, немає підстав сумніватися в можливості настільки ж успішного впровадження механізмів безпеки в Internet-системи. Додатковою перевагою такого підходу буде можливість атестації таких систем відповідно до діючого законодавства. У цьому випадку WWW-сервер використає механізм екранування сервисів для створення незалежного засобу доступу й блокування дії програмних закладок у ПО сервера баз даних.

Основними компонентами брандмауера є:

- політика мережного доступу;
- механізми посиленої автентифікації;
- фільтрація пакетів;
- прикладні шлюзи.

Можливі різні конфігурації брандмауерів:

- брандмауер з пакетною фільтрацією;
- брандмауер зі шлюзом із двома адресами;
- брандмауер з екранованим хостом;
- брандмауер з екранованою мережею;
- інші.

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1: Ознайомитись з типами політик мережного доступу, технічної реалізації цих політик, вибір типів міжмережних екранів для забезпечення безпеки ЛОМ, порядок їх реалізації і технічної експлуатації

Брандмауер виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;
- ідентифікацію запитів, що надходять в мережу, в декілька етапів;
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;

- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі;
- приховування IP-адреси внутрішніх серверів з метою захисту від хакерів.

Розрізняють два типи МЕ: **апаратний і програмний**. **Апаратний** являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер**. Програмний** виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп'ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип МЕ.

МЕ можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP-адресам: не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено. На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

МЕ розділяють на **три види**:

- пакетні фільтри (packet filter);
- сервера прикладного рівня (application gateways);
- сервера рівня з'єднання (circuit gateways).

МЕ з пакетними фільтрами приймають рішення про те чи пропускати пакет, чи відкинути, переглядаючи IP-адреси, прапорці або номери TCP портів в заголовку цього пакета. IP-адреса та номер порту – це інформація мережевого і транспортного рівнів. Водночас, пакетні фільтри використовують також інформацію прикладного рівня, тобто всі стандартні сервіси в TCP/IP асоціюються з певним номером порту.

Переваги пакетних фільтрів: відносно невисока вартість; гнучкість у визначенні правил фільтрації; невелика затримка при проходженні пакетів.

Недоліки: локальна мережа стає видима з мережі Internet; правила фільтрації пакетів важкі в описі, потрібні дуже хороші знання технологій TCP і UDP; при порушенні працездатності МЕ всі комп'ютери стають повністю незахищеними або недоступними; аутентифікацію з використанням IP-адреси можна обдурити використанням IP-спуфінга (атакуюча система видає себе за іншу, використовуючи її IP-адресу); відсутня аутентифікація на рівні користувача.

МЕ прикладного рівня використовують сервера конкретних сервісів: TELNET, FTP і т.д. Proxy—server, що відносяться до даного сервісу, запускаються на екрані та пропускають через себе весь трафік. Між клієнтом і сервером утворюються два з'єднання: від клієнта до МЕ і від нього до місця

призначення. Використання серверів прикладного рівня дозволяє вирішити важливе завдання**:** приховати від зовнішніх користувачів структуру локальної мережі, включаючи інформацію в заголовках поштових пакетів або служби доменних імен (DNS).

Переваги серверів прикладного рівня: локальна мережа стає невидимою з мережі Internet; при порушенні працездатності між мережевого екрана пакети перестають проходити через нього, тим самим не виникає загрози для захисту локальної мережі; захист серверів прикладного рівня дозволяє здійснювати велику кількість додаткових перевірок, знижуючи тим самим імовірність злому з використанням дірок у програмному забезпеченні; за допомогою аутентифікації на рівні користувача може бути реалізована система негайного попередження про спробу злому.

Недоліки: більш висока вартість, продуктивність нижча ніж у пакетних фільтрів; неможливість використання протоколів RPC і UDP.

Сервер рівня з'єднання схожий на МЕ прикладного рівня тим, що вони обидва є серверами-посередниками. Користувач утворює з'єднання з певним портом на екрані, після чого останній з'єднюється з місцем призначення по іншу сторону від МЕ. Використовуючи різні порти, можна створювати різні конфігурації. Такий тип сервера дозволяє створювати канал зв'язку для будь-якого сервісу, що базується на TCP, здійснювати контроль доступу до цього сервісу, збір статистики щодо його використання.

Головна відмінність між ними полягає в тому, що МЕ прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, МЕ рівня з'єднання обслуговують велику кількість протоколів. Але МЕ не можуть повністю гарантувати безпеку даних у локальних комп'ютерних мережах, тому що не можуть запобігти виникненню таких проблем як: віруси, що поширюються електронною поштою та фішингове шахрайство.

Міжмережевий екран пропускає через себе весь трафік, приймаючи щодо кожного пакету, що рішення: дати йому можливість пройти чи ні. Для того щоб міжмережевий екран міг здійснити цю операцію, йому необхідно визначити набір правил фільтрації. Рішення про те, фільтрувати чи за допомогою брандмауера конкретні протоколи і адреси, залежить від прийнятої в мережі, що захищається політики безпеки. Міжмережевий екран являє собою набір компонентів, що настроюються для реалізації обраної політики безпеки.

Політика мережевої безпеки кожної організації повинна включати дві складові:

1. Політика доступу до мережевих сервісів.
2. Політика реалізації міжмережевих екранів.

Політика доступу до мережевих сервісів повинна бути уточненням загальної політики організації щодо захисту інформаційних ресурсів в організації. Для того щоб міжмережевий екран успішно захищав ресурси організації, політика доступу користувачів до мережевих сервісів повинна бути реалістичною. Такий вважається політика, при якій знайдений гармонійний баланс між захистом мережі організації від відомих ризиків і необхідністю

доступу користувачів до мережевих сервісів. Відповідно до прийнятої політики доступу до мережевих сервісів визначається список сервісів Інтернету, до яких користувачі повинні мати обмежений доступ. Задаються також обмеження на методи доступу, необхідні для того, щоб користувачі не могли звертатися до заборонених сервісів Інтернету обхідними шляхами.

Міжмережевий екран може реалізувати ряд політик доступу до сервісів. Але зазвичай політика доступу до мережним сервісів заснована на одному з таких принципів:

1. Заборонити доступ з Інтернету у внутрішню мережу і дозволити доступ з внутрішньої мережі в Інтернет.
2. Дозволити обмежений доступ у внутрішню мережу з Інтернету, забезпечуючи роботу тільки окремих авторизованих систем, наприклад інформаційних і поштових серверів.

Відповідно до політики реалізації міжмережевих екранів визначаються правила доступу до ресурсів внутрішньої мережі. Перш за все необхідно встановити, наскільки «довірчої» чи «підозрілою» повинна бути система захисту. Іншими словами, правила доступу до внутрішніх ресурсів повинні базуватися на одному з наступних принципів:

1. Забороняти все, що не дозволено в явній формі.
2. Вирішувати все, що не заборонено в явній формі.

Ефективність захисту внутрішньої мережі за допомогою міжмережевих екранів залежить не тільки від обраної політики доступу до мережевих сервісів і ресурсів внутрішньої мережі, але і від раціональності вибору і використання основних компонентів мережевого доступу.

Основні способи розгортання міжмережевих екранів в корпоративних мережах при підключенні корпоративної або локальної мережі до глобальних мереж адміністратор мережевої безпеки повинен вирішувати такі завдання:

захист корпоративної або локальної мережі від несанкціонованого віддаленого доступу з боку глобальної мережі;

приховування інформації про структуру мережі та її компонентів від користувачів глобальної мережі;

розмежування доступу в мережу, що захищається з глобальної та з мережі, що захищається в глобальну.

Завдання 2: Знайомство з комплексом засобів міжмережного екрану Agnitum Outpost Firewall (програмної та апаратної частин), встановленого на ОС MS WINDOWS

Outpost Firewall Free - безкоштовний фаєрвол, для захисту персонального комп'ютера від хакерських атак. Крім захисту від зовнішнього проникнення з мережі, Outpost Firewall Free дозволяє проводити захист від нелегального витоку конфіденційної інформації за допомогою встановлених на комп'ютері програм (https://biblprog.org.ua/ru/outpost_firewall/).

Для виконання даної лабораторної роботи, за бажанням, можна використовувати Comodo Firewall (Free Firewall/Download Comodo Award Winning Free Firewall https://www.comodo.com/home/internet-security/firewall.php)

1. Відкрийте програму Outpost Firewall. Вивчіть функціональні можливості вкладок контекстного меню «Параметри».

2. Налаштуйте функції програми Outpost Firewall, залежно від вимог, зазначених у вашому варіанті (рис. 5.1).

3. Налаштуйте журнал програми Outpost Firewall для відображення тільки необхідної інформації, обумовленої вашим завданням.

Брандмауер дозволяє налаштовувати фільтри, що відповідають за пропуск трафіку за наступними критеріями:

1. **IP-адреса**. Як відомо, будь-яке кінцеве пристрій, що працює по протоколу IP, повинно мати унікальну адресу. Задавши якусь адресу або певний діапазон, можна заборонити отримувати з них пакети, або, навпаки, дозволити доступ тільки з даних IP-адрес.

2. **Доменне ім'я**. Як відомо, сайту в мережі Інтернет, точніше його IP-адресою, може бути поставлено у відповідність буквено-цифрове ім'я, яке набагато простіше запам'ятати, ніж набір цифр. Таким чином, фільтр може бути налаштований на пропуск трафіку тільки до / від одного з ресурсів, або заборонити доступ до нього.

3. **Порт.** Йдеться про програмні портах, тобто точках доступу додатків до послуг мережі. Так, наприклад, ftp використовує порт 21, а додатки для перегляду web-сторінок порт 80. Це дозволяє заборонити доступ з небажаних сервісів і додатків мережі, або, навпаки, дозволити доступ тільки до них.

4. **Протокол**. Брандмауер може бути налаштований на пропуск даних тільки якого-небудь одного протоколу, або заборонити доступ з його використанням. Зазвичай тип протоколу може говорити про виконувані завдання використовуваного ним програми та про набір параметрів захисту. Таким чином, доступ може бути налаштований тільки для роботи якого-небудь одного специфічного додатки і запобігти потенційно небезпечний доступ з використанням всіх інших протоколів.

Основні етапи налаштування міжмережного екрана

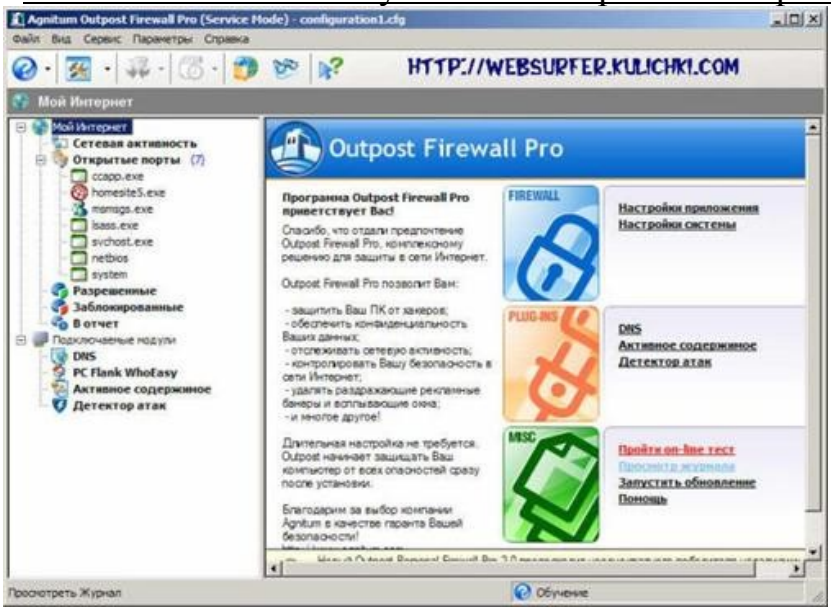

Рис.5.1. Вікно програми Outpost Firewall

Закладка – загальні (рис. 5.2). У самому верху вікна опція - завантаження й три варіанти на вибір - звичайний, фоновий і не завантажувати. За замовчуванням встановлено перший варіант.

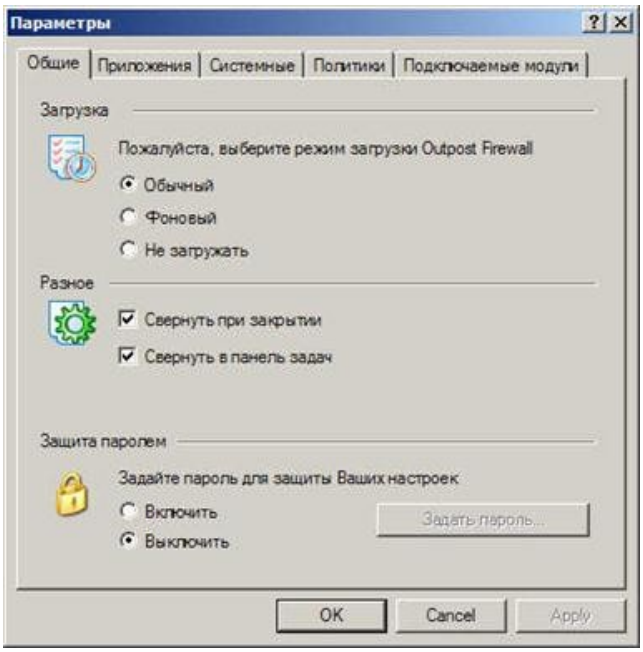

Рис.5.2 Установчі параметри Outpost Firewall

Закладка – додатки (рис. 5.3). У цьому вікні будуть з'являтися програми в міру їхнього першого запуску й виходу в мережу. Діляться додатки (мається на увазі програми) на три категорії - заборонені, користувальницький рівень і дозволені. Заборонені - це ті програми, яким адміністратор заблокував доступ до інтернету;до користувальницького рівня відносяться ті програми, для яких адміністратор склав певні правила використання мережі (тобто не все можна, а тільки певні дії) і нарешті останній варіант - це дозволені програми, тобто ті, котрим дозволено все (мається на увазі, що використати мережу вони можуть як завгодно).

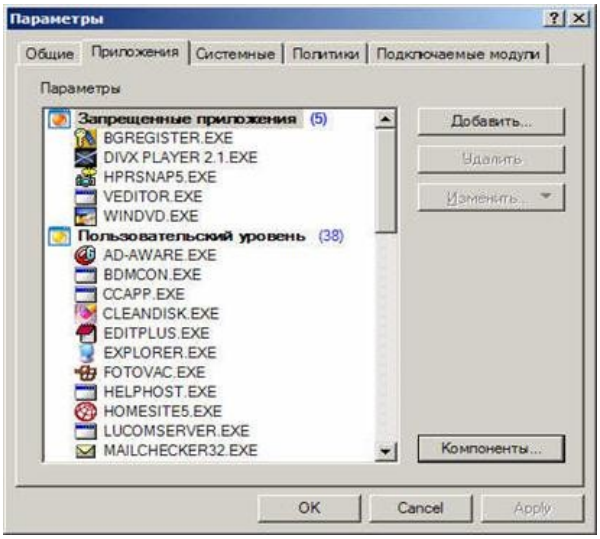

Рис.5.3 Додатки Outpost Firewall

Кнопка “компоненти” відображає всі складові програм із цього вікна - динамічні бібліотеки, запущені файли, тобто всі ті компоненти програм, які власне кажучи й використовують мережу (рис.5.4, 5.5).

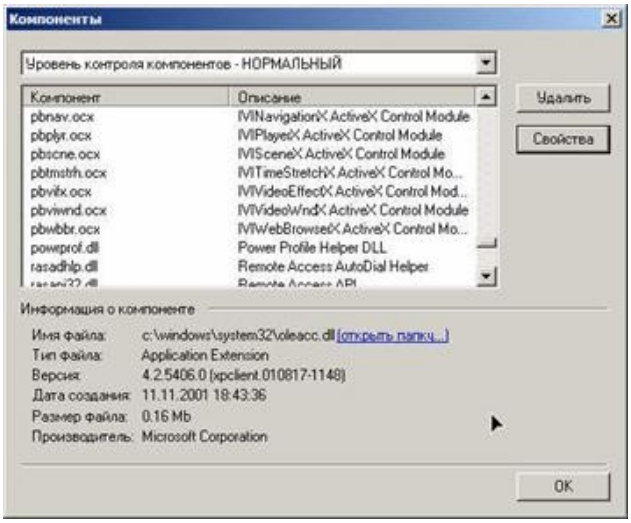

Рис.5.4 Компоненти Outpost Firewall

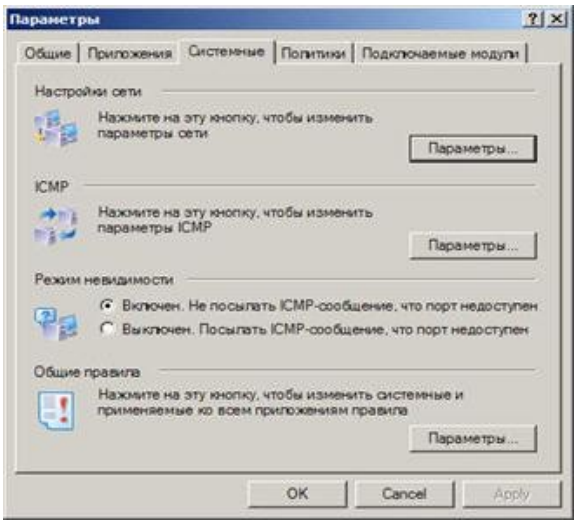

Рис.5.5. Мережеві налаштування

Закладка - системні. Сюди входять - налаштування мережі (рис. 5.6), ICMP (Internet Control Message Protocol) використовується, щоб посилати повідомлення про помилки керування між комп'ютерами, зв'язаними за мережею (рис. 5.7). Ці параметри встановлені за замовчуванням. Далі секція - режим невидимості. Тут два варіанти - включений/виключений, за замовчуванням цей режим включений.

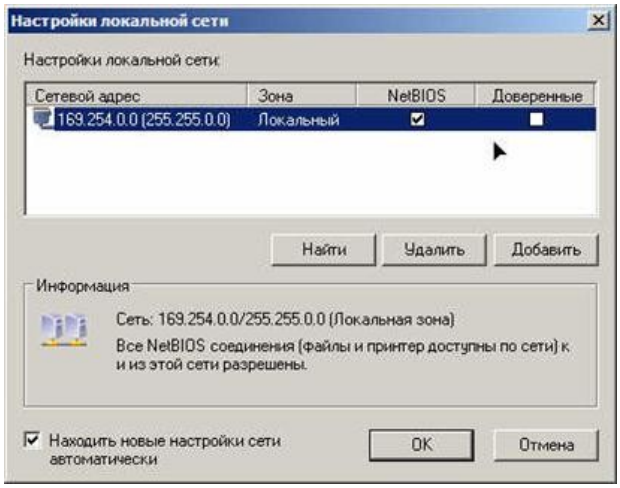

Рис.5.6. Налаштування ЛОМ

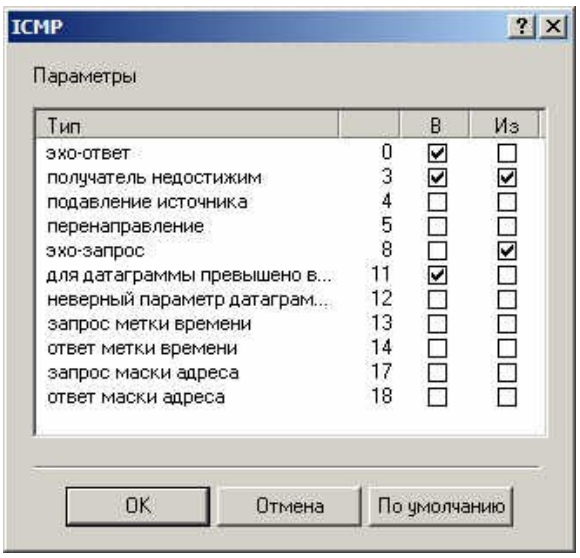

Рис.5.7. Налаштування Internet Control Message Protocol

У цьому вікні можна побачити встановлені правила використання мережі, сюди ж можна додавати й свої правила. і це буде відноситись до варіанта програм користувальницького рівня.

Варіанти завдань для виконання лабораторної роботи № 5

(Налаштування параметрів Outpost Firewall):

1. На робочих комп'ютерах користувачів необхідно блокувати відображення в браузерах рекламних банерів, а також повідомляти користувачів про сканування їхнього комп'ютера, навіть якщо було зафіксовано одноразове сканування.

2. Робочі комп'ютери користувачів необхідно настроїти, заборонивши відображення на Web-Сторінках елементів ActiveX, а також реалізувати блокування атакуючого вузла, при виявленні підозри на здійснення атаки.

3. На робочих комп'ютерах користувачів необхідно блокувати доступ до Web-Сайтів, що містять слова з певного списку, а також реалізувати автоматичне блокування підмережі, з якої вироблялися спроби атак.

4. На робочих комп'ютерах користувачів необхідно дозволити виконання Java і VB сценаріїв, а також реалізувати запобігання підміни ARP-адрес,

приймаючи тільки ті відповіді, для яких була відправлена адреса.

5. На робочих комп'ютерах користувачів необхідно блокувати показ інтерактивних рекламних оголошень, що відображаються в браузері. А також, реалізувати виявлення підміни IP-адреси й блокувати атаку.

6. На робочих комп'ютерах користувачів, необхідно заблокувати можливість відкривати деякі Web-Сторінки, а також реалізувати запобігання помилкових повідомлень «IP-адреса вже зайнята».

7. На робочих комп'ютерах користувачів необхідно заборонити показ браузерами Java-апплетов, а також настроїти час після якого, необхідно блокувати DoS атаки.

8. На робочих комп'ютерах користувачів необхідно настроїти фільтрацію .exe-файлів, що надходять електронною поштою, а також настроїти список системних портів, за яких програма повинна спостерігати, з підвищеною увагою, для виявлення атак.

9. На робочих комп'ютерах користувачів необхідно настроїти функцію, при якій робота з cookies буде здійснена тільки за згодою користувача, а також указати вилучені вузли й порти довірчих комп'ютерів, які не будуть розглядатися як шкідливі.

10. На робочих комп'ютерах користувачів необхідно настроїти фільтрацію *.bat-файлів, що надходять електронною поштою, а також налаштувати список «троянських» портів, за якими програма повинна спостерігати, з підвищеною увагою, для виявлення атак.

11. На робочих комп'ютерах користувачів необхідно заборонити відображення в браузерах спливаючих вікон, а також реалізувати перевірку й блокування невірних DNS запитів та блокування наддовгих DNS запитів.

12. На робочих комп'ютерах користувачів необхідно блокувати відображення в браузерах рекламних оголошень стандартних розмірів, а також реалізувати виявлення підміни MAC-адреси й блокувати атаку.

Порядок і рекомендації щодо виконання роботи

1. Надати до Звіту з лабораторної роботи докладний опис функцій, які ви набудовували для рішення поставленого завдання. Обґрунтуйте вибір настроювань, які ви використовували для рішення завдання.

2. Внесіть до Звіту з лабораторної роботи результат роботи програми й пророблені вами настроювання журналу.

3. Дайте відповідь на контрольні питання:

1). Опишіть призначення міжмережних екранів. Які функції виконує програма Outpost Firewall?

2). Поясніть функціональне призначення вкладок вікна «Параметри».

3). Для чого служать «Політики» Outpost Firewall? Опишіть призначення існуючих у програмі Outpost Firewall політик.

4). На які групи й для яких цілей розділяються додатки системи впрограмі Outpost Firewall?

5). Які дії необхідно зробити для переносу додатка з однієї групи в іншу?

6). Опишіть функції визначених правил у програмі Outpost Firewall.
7). Які дії необхідно зробити для формування користувальницьких правил?
8). Які умови можна сформувати для протоколів? Опишіть призначення цих умов і протоколів.
9). Опишіть процес настроювання системних протоколів. Які параметри настроювання можна вибрати, яке функціональне призначення даних параметрів?
10). Для чого служать модулі, що підключаються? Опишіть роботу з ними.
11). Дайте визначення терміну: “брандмауер”.
12). Назвіть основні типи брандмауерів

4. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

– відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.
3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_01_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп’ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.
2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.
4. Кузнецов О.О. Захист інформації в інформаційних системах. Вид. ХНЕУ, 2017. 286 с.

Лабораторна робота № 6 (4 години)

Тема: Методика побудови захищеної телекомунікаційної мережі із використанням VPN

Мета роботи: проведення аналізу протоколів, що застосовуються у віртуальних приватних мережах для вирішення завдання вибору оптимального рішення віддаленого доступу до внутрішніх ресурсів корпоративної мережі.

Мета виховна: виховання свідомого ставлення до праці та навчання, розвиток розумових здібностей, високих моральних якостей,

самовдосконалення, індивідуальних здібностей.

Завдання

1. Огляд наявних рішень, присутніх на ринку технологій VPN.
2. Налагодження підключення до віртуальної приватної мережі (VPN) в Windows XP

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі, обладнане ПК із встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації

Короткий теоретичний коментар до теми

VPN виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;
- ідентифікацію запитів, що надходять в мережу, в декілька етапів;
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі;
- приховування IP-адреси внутрішніх серверів з метою захисту від хакерів.

Розрізняють два типи МЕ: **апаратний і програмний**. **Апаратний** являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер**. Програмний** виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп'ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип реалізації МЕ.

МЕ можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP-адресам: не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено. На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний,

синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1: Огляд наявних рішень, присутніх на ринку технологій VPN.

1. Зробити аналітичний огляд технологій VPN, які використовуються на даний час (загалом) та є найбільш вживаними, з урахуванням вітчизняного та зарубіжного ринків.

2. Аналіз представити у вигляді графіків/діаграм

Завдання 2: Налагодження підключення до віртуальної приватної мережі (VPN) в Windows XP

1. Натисніть кнопку "Пуск"→"Панель управління" або **"Пуск"→** "Налаштування"→**"Панель управління"**.

Якщо ваша Панель управління має такий вигляд, необхідно зліва натиснути "Переключення до класичного вигляду". На панелі управління двічі натисніть значок "Мережеві підключення" (рис. 6.1).

Архітектурно Internet-системи являють собою трирівневі системи “клієнт-сервер” з використанням WWW-сервера в якості ПО як проміжного шару. Оскільки саме трирівневі системи звичайно використовуються для найбільш ефективної роботи механізмів безпеки, немає підстав сумніватися в можливості настільки ж успішного впровадження механізмів безпеки в Internet-системи.

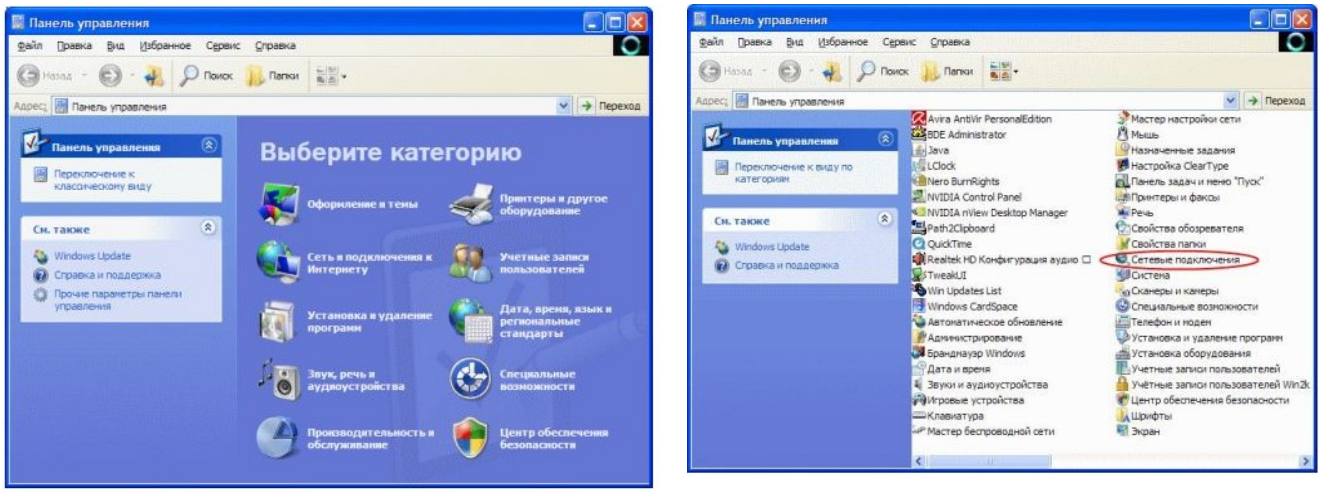

Рис. 6.1 Виклик Панелі управління та "Мережеві підключення"

Додатковою перевагою такого підходу буде можливість атестації таких систем відповідно до діючого законодавства. У цьому випадку WWW-сервер використає механізм екранування сервисів для створення незалежного засобу доступу й блокування дії програмних закладок у ПО сервера баз даних.

Порядок і рекомендації щодо виконання роботи

1. Вивчити теоретичні відомості по можливостям захисту VPN.

2. Надати наочні результати аналізу технології VPN та результати налаштування віртуальної приватної мережі у вигляді скріншотів з поясненням виконання кожного кроку налаштування.
3. Дати відповідь на контрольні питання:
4. З яких дій складається процедура генерації ключів?
5. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

– відповіді на запитання (п. 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.
3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_06_**Прізвище_Ініціали***), який містить файл зі звітом.

Список рекомендованої літератури

1. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах. навч. посіб. Х.: НТУ «ХПІ», 2015. 251 с.
2. Хорошко В. О. Проєктування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Петренко В.И., Мандрица И.В. Защита персональних даннях в информационных системах. Практикум. Издательство: Лань, 2019. 687 с.

Лабораторна робота № 7 (4 години)

Тема: Криптографічні методи захисту даних: проста перестановка по ключу, подвійна перестановка, магічні квадрати

Мета навчальна: використання криптографічного захисту інформації під час побудови політики безпеки on-line-системи при використанні безпечної системи розподілу криптографічних ключів

Мета виховна: сприяти розвитку компетентності в галузі використання інформаційно-комунікаційних технологій, навчити співпрацювати в групі, незалежно від інтелектуальних і творчих здібностей; виховувати відповідальність і самостійності при виконанні практичних та творчих завдань

Завдання:

1. Виконати шифрування повідомлення за зразком, використовуючи метод простої перестановки по ключу, подвійної перестановки та метод магічних квадратів.
2. Зашифрувати текстове повідомлення, згідно з варіантами, призначеними викладачем, користуючись вивченими методами шифрування.

Перелік спеціального обладнання та устаткування: індивідуальне робоче місце в комп'ютерному класі обладнане ПК із підключенням до мережі Internet, встановленою версією операційної системи, пакетом стандартних програм, браузерами та відведене місцем для збереження інформації, мультимедійний проектор.

Короткий теоретичний коментар до теми

1. Проста перестановка по ключу

Ключем для шифрування-розшифрування служить розмір таблиці і ключове слово. Повідомлення записується в таблицю по стовпцях, а для формування шифротексту вміст таблиці прочитується по рядках. Метод шифрування полягає в тому, що стовпці таблиці переставляються по ключовому слову, фразі або набору чисел завдовжки в рядок таблиці.

При дешифруванні текст записується в таблицю по рядках, потім стовпці переставляються відповідно до ранжування ключового слова, далі текст читається по стовпцях.

2. Подвійна перестановка

Для додаткової потаємності можна повторно зашифрувати повідомлення, яке вже було зашифровано. Цей спосіб відомий під назвою подвійна перестановка. Для цього розмір другої таблиці підбирають так, щоб довжина її рядків і стовпців були інші, ніж у першій таблиці. Краще всього, якщо вони будуть взаємно простими. Крім того, в першій таблиці можна переставляти стовпці, а в другій рядки. Спочатку повідомлення записується в таблицю по стовпцях, потім по черзі переставляються стовпці, а потім рядки. При дешифруванні порядок перестановок повинен бути зворотним. Такі способи заповнення таблиці якщо і не посилюють стійкість шифру, то роблять процес шифрування набагато більш цікавим.

Для дешифрування порядок перестановок повинен бути зворотним, тобто спочатку переставляють рядки, потім стовпці.

Число варіантів подвійної перестановки швидко зростає при збільшенні розміру таблиці:

- для таблиці 3x3 - 36 варіантів;
- для таблиці 4x4 - 576 варіантів;
- для таблиці 5x5 - 14400 варіантів.

Проте подвійна перестановка не відрізняється високою стійкістю і порівняно просто "зламуються" при будь-якому розмірі таблиці шифрування.

3. Магічні квадрати

Магічними квадратами називають квадратні таблиці з вписаними до них клітини послідовними натуральними числами, починаючи від 1, які дають у сумі по кожному стовпцю, кожному рядку і кожній діагоналі одне й те саме число (наприклад, 16+3+2+13=34 і т. д). Текст, який шифрується, вписували до магічних квадратів відповідно до нумерації їх клітин. Відкритий текст вписується в магічний квадрат відповідно до нумерації кліток., прочитавши який по рядках, одержимо шифротекст.

Методи навчання

Словесні (пояснення, інструктаж); наочні (демонстрація, ілюстрування) практичні (лабораторна робота); за логікою (індуктивний, аналітичний, синтетичний, порівняння) за мисленням (дослідницький, репродуктивний).

Порядок та методика виконання завдань лабораторної роботи

Завдання 1. Виконати шифрування повідомлення за зразком, використовуючи метод простої перестановки по ключу, подвійної перестановки та метод магічних квадратів.

1. Виконати просту перестановку по ключу:

1.1. Візьмемо повідомлення: ПЕРЕСТАНОВКА. Застосуємо як ключ слово: ШИФР

← порядок літер в алфавіті

П			
Е			
Р			

			4
			П
			Е
			Р

Одержуємо шифротекст: ЕВАПСКНЕТАОР

1.2. Відкритий текст: ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ

Ключ (правило перестановки): групи з 8 букв с порядковими номерами 1,2.....8 переставити в порядок 3-8-1-5-2-7-6-4.

Отримуємо шифротекст: "ФНШОИАВР_СИЕЕЕРПННТВАОКО"

2. Подвійна перестановка: Ключем до шифру подвійної перестановки служить послідовність номерів стовпців і номерів рядків початкової таблиці, для нижченаведеного прикладу: (4 1 3 2) і (3 1 2)

Наприклад, відкритий текст: ПЕРЕСТАНОВКА

Вихідна таблиця

Перестановка стовпців

Перестановка рядків

Шифротекст: СЬКНЕ ТАОР ЕВАП

3. Магічні квадрати

Відкритий текст: ШИФР ПЕРЕСТАНОВКИ. Використовуємо один з магічних квадратів розміром 4х4:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

И	Ф	И	О
П	Т	А	Е
С	Е	Р	Н
Р	К	В	Ш

Шифротекст: ИФИО ПТАЕ СЕРН РКВШ

Завдання 2: Зашифрувати текстове повідомлення, згідно з варіантами, призначеними викладачем, користуючись вивченими методами шифрування

№ варіанту	Метод шифрування	Початкові параметри
1	Проста перестановка по	Розмір таблиці, ключове слово або
2	Подвійна перестановка.	Розмір таблиці, перестановки стовпців і рядків.
3	Шифрування з використанням магічного квадрата.	Розмір квадрата, нумерація кліток

Завдання для самостійної роботи

1. Алгоритм – чітко задана послідовність кроків для розв’язання завдання.
2. Інформація - це дані про явища, процеси та предмети навколишнього середовища
3. Інсталяція - це процес установки програмного забезпечення на комп’ютер користувача.
4. Комп’ютерна мережа — це сукупність комп’ютерів і периферійного обладнання.
5. Обчислювальна мережа — це складний комплекс взаємозалежних програмних і апаратних компонентів.
6. Модератори - люди, які постійно стежать за дотриманням порядку на форумах.
7. Програма - план дій, який підлягає виконанню певним виконавцем.
8. Моделювання – це процес створення і дослідження моделі.
9. Інтерфейс – це прості та зручні засоби взаємозв’язку між користувачем та програмою.
10. Криптографія – наука про способи перетворення інформації (шифрування) з метою її захисту.
11. Макрос – це записана під певним іменем послідовність дій або команд.
12. Форматування – це процес розбивки диска на сектори і доріжки засобами операційної системи.
13. Де фрагментація — це оптимізація дискового простору, упорядкування кластерів, які належать одному файлу.
14. Кластер — це група логічно послідовних секторів на диску.

15. Оперативна пам'ять призначена для збереження поточних даних і виконуваних програм.
16. Контролер – це пристрій керування периферійним устаткуванням.
17. Відеосистема ПК – складається з відеоадаптера (графічної плати) і дисплея (монітора).
18. Утиліта – допоміжна програма для розширення можливостей ОС
19. Шлюз – електронний пристрій і відповідне програмне забезпечення
20. Дисплей – пристрій візуалізації текстової і графічної інформації

Порядок і рекомендації щодо виконання роботи

1. У звіті до лабораторної роботи надати виконане завдання з шифрування індивідуального повідомлення з описом методів шифрування, які представлені в даній лабораторній роботі .
2. Дайте відповідь на контрольні питання.
   1) Що є ключем для шифрування-розшифрування в простій перестановці по ключу?
   2) Що служить ключем до шифру подвійної перестановки?
   3) Що таке «магічні квадрати»?
   4) Які основні принципи шифрування простою перестановкою по ключу ?
   5) Які основні принципи шифрування методом подвійної перестановки?
3. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту лабораторної роботи

1. У звіті до даної роботи повинні міститися:

– № лабораторної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

– результати виконання завдань № 1,2;

– відповіді на запитання (п. 2 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному вигляді у форматі *.odf, *.doc або *.docx.
3. Надіслати викладачу листа з архівом (файл назвати БІС_Lab_07_**Прізвище_Ініціали***), який містить файл зі звітом.

Список використаних джерел

1. Щербаков Л. Ю., Домашен А. В. Прикладная криптография. Использование и синтез крипторафических интерфейсов. М: Издательско-торговый дом Русская Редакциям, 2015. 416 с.
2. С.Г. Баричев и др. Основы современной криптографии. М.: Горячая линия-Телеком, 2018. 60 с.
3. Семенюк В.В. Экономное кодирование дискретной информации. СПб.: СПбГИТМО (ТУ), 2017. 115с.

Підписано до друку _____
Формат 84х60/16. Гарнітура Таймс.
Друк – різографія. Папір офсетний.
Ум.друк.арк. 1,625***. обл. Вид арк.. ***. Наклад 50 прим.***
ПП ПДАУ, вул. Сковороди, 1/3, м. Полтава,36003