МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

АПАРАТНІ ТА ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання

Луцьк 2025

УДК 004.056(075.8)+681.518(075.8)
А76

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № ___ від _____ 2025 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладачі: _____ Олег КАЙДИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Сергій ГРИНЮК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

А76 Апаратні та програмні засоби захисту інформації: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 68 с.

У пропонованому виданні містяться матеріали до лабораторних занять з курсу «Апаратні та програмні засоби захисту інформації».

Методичні вказівки покликані зосередити увагу здобувачів освіти на основних методах та технологіях захисту інформації, допомагають краще усвідомити принципи роботи апаратних і програмних засобів захисту інформації та стимулюють критичне мислення й аналітичні їх здібності під час різних життєвих ситуації, які можуть виникнути під час загрози безпеці.

ВСТУП

На сьогодні захист інформації є однією із найактуальніших задач, адже широкого розповсюдження набувають системи оброблення інформації. Розширення локальних та глобальних комп'ютерних мереж дозволяє передавати великі об'єми інформації різного характеру, при цьому її власники не готові оприлюднювати деяку інформацію для сторонніх осіб. Це спонукає до формування певної проблеми, яка зобов'язує зберігати та передавати інформацію в інформаційній системі лише у захищеному вигляді.

Розширення комп'ютерних мереж та обробка великих обсягів даних призводить до зростання ризику кібератак. При цьому організація або установа повинна бути готовою до реагування на такі інциденти.

З поміж усіх існуючих технологій, які використовуються для захисту даних, доцільно виділити шифрування, системи контролю доступу, антивірусні програми, брандмауери тощо. Варто пам'ятати, що важливим залишається й питання впроваджування регулярних аудитів безпеки та навчання персоналу.

Лабораторні роботи з курсу «Апаратні та програмні засоби захисту інформації» є важливою складовою навчального процесу та покликані набути здобувачами освіти практичних навичок під час використання найрізноманітних апаратних і програмних засобів захисту інформації. Ідентифікування потенційних загроз, аналіз вразливості систем, розроблення стратегії для їх усунення допоможуть для них розробляти власні рішення, які будуть спрямовані на захист інформації, що дозволить розвинути у них творче мислення та інженерні навички.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА №1

Тема: шифр Цезаря.

Мета: розробити криптосистему на основі шифру Цезаря.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Шифр Цезаря – один із найдавніших шифрів, названий на честь римського імператора Гая Юлія Цезаря, який використовував його для секретного листування. Під час шифрування кожен символ замінюється іншим, віддаленим від нього в алфавіті на фіксоване число позицій.

Якщо співставити кожному символу абетки його порядковий номер, то шифрування й розшифрування можна виразити через вираз (1.1) модульної арифметики:

$$y=(x+k)x \bmod n=(y+n-(k \bmod n))\bmod n, \qquad (1.1)$$

де x – символ відкритого тексту;

y – символ шифрованого тексту;

n – потужність абетки;

k – ключ.

З прикладами використання шифру Цезаря можна ознайомитись на наступних сайтах:

- https://findhow.org/5069-shifr-tsezarya.html;
- http://hostciti.net/calc/it/cipher-ceaser.html;
- https://codepen.io/andrey18106/pen/ZjyXdz.

ХІД РОБОТИ

1. Розробити інтерфейс криптографічної системи симетричного шифрування, передбачивши у ньому використання меню та/або панелі інструментів для виконання наступних команд:

- створення, відкривання, збереження, друк файлів;
- шифрування та розшифрування файлів українською та англійською мовами;
- вихід із системи.

2. Розробити систему класів для реалізації симетричного шифрування методом Цезаря, передбачивши в них методи валідації ключа, валідації, шифрування і розшифрування даних.

3. Виконати тестування роботи системи.

4. Додаткові завдання:

– доповнити розроблену систему модулем для атаки на шифр Цезаря методом «грубої сили» (перебору);

– розширити можливості системи, забезпечивши можливість шифрування даних в будь-якому форматі, а не тільки текстових.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Криптографія та предмет її вивчення.
2. Які властивості інформації захищають криптографічними засобами?
3. Що являє собою ключ шифрування?
4. Формула модульної арифметики: призначення та суть.
5. Як здійснюється шифрування за допомогою модифікованого шифру Цезаря?

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №2

Тема: шифр Тритеміуса.

Мета: розробити криптосистему на основі шифру Тритеміуса.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Шифр Тритеміуса – вдосконалений шифр Цезаря, в якому кожен символ повідомлення зміщується на символ, який відстає від даного на деякий крок. Але крок зміщення робиться змінним, тобто залежним від будь-яких додаткових чинників. Наприклад, можна задати закон зміщення у вигляді лінійної функції позиції літери, що шифрується, або за допомогою використання гасла – текстового рядка, який багаторазово записується під текстом повідомленням.

Таким чином, шифрування і розшифрування для шифру Тритеміуса можна виразити за допомогою рівняннь (2.1) та (2.2) відповідно:

$$y=(x+k) \bmod n; \quad (2.1)$$

$$x=(y+n-(k \bmod n)) \bmod n, \quad (2.2)$$

де x – символ відкритого тексту;

y – символ шифрованого тексту;

n – кількість літер абетки.

Крок зміщення k прийнято розраховувати:

– за лінійним рівнянням: $k=A_p+B$;
– за нелінійним рівнянням: $k=A^2+B_p+C$;
– за гаслом.

Тут у якості p виступає позиція літери в повідомленні. Ключем шифрування виступають відповідно коефіцієнти вказаних рівнянь та гасло.

З прикладами використання шифру Тритеміуса можна ознайомитись на наступних сайтах:

– http://surl.li/svxac;
– http://surl.li/svxbw.

ХІД РОБОТИ

1. Модифікувати інтерфейс криптографічної системи симетричного шифрування за шифром Цезаря (на основі створеної в лабораторній роботі №1 системи), забезпечивши можливість використання в якості ключа:

– двовимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування;

– трьохвимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування;

– текстового рядка (гасла).

2. Доповнити систему класів криптографічної системи симетричного шифрування за шифром Цезаря (на основі створеної в лабораторній роботі №1 системи) класами та методами, які є необхідними для реалізації симетричного шифрування методом Тритеміуса, передбачивши у них методи валідації ключа, валідації шифрування і розшифрування даних.

3. Виконати тестування роботи системи.

4. Додаткові завдання:

– доповнити систему модулем активної атаки на шифр Тритеміуса, який би забезпечував знаходження ключа шифрування у випадку, коли зловмиснику вдалось отримати пару повідомлень «незашифроване-зашифроване;

– доповнити розроблену систему модулем для атаки на шифр Цезаря методом «грубої сили» (перебору).

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Архітектура криптографічної системи.
2. Що таке шифр? Які шифри називають історичними?
3. Яким виразом можна описати шифрування та розшифрування для шифру Тритеміуса.

4. Класифікація алгоритмів шифрування.
5. Ключ шифрування.

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №3

Тема: шифр гамування.

Мета: розробити криптосистему на основі шифру гамування.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Даний метод полягає в тому, що символи тексту, який шифрується, послідовно складаються із символами деякої спеціальної послідовності, яка називається гамою. Іноді такий метод представляють як накладення гами на вхідний текст, тому він отримав назву «гамування». При цьому символи вихідного тексту і гамми замінюються цифровими еквівалентами, які потім складаються по модулю n (де n – число символів в абетці), тобто шифрування й розшифрування для шифру гамування можна виразити рівняннями (3.1) та (3.2) відповідно:

$$y=(x+g) \bmod n; \tag{3.1}$$

$$x=(y+n-(g \bmod n)) \bmod n, \tag{3.2}$$

де x – символ відкритого тексту;

y – символ шифрованого тексту;

g – символ гами.

Найбільш часто, на практиці, зустрічається двійкове гамування. При цьому використовується двійкова абетка, а складання здійснюється за модулем два (3.3):

$$z=x+g(\bmod 2)=x \text{ XOR } g. \tag{3.3}$$

Операція складання по модулю два в алгебрі логіки називається також «виключне АБО» або XOR (з англійської) та позначається сиволом «$\oplus$».

Операція XOR дуже швидко виконується на комп'ютері (на відміну від багатьох інших арифметичних операцій), тому накладення гами навіть на дуже великий відкритий текст виконується практично миттєво.

Цю ж саму операцію використовують і для розшифрування.

Під час використання методу гамування ключем є послідовність, з якою проводиться складання – гамма. Якщо гамма коротша за повідомлення, яке було призначене для шифрування, гамма повторюється необхідну кількість разів. Чим довший ключ, тим надійніше шифрування методом гамування.

На практиці розрізняють два різновиди гамування: з кінцевою і нескінченною гамами. За умови хороших статистичних властивостей гами якість шифрування визначається тільки довжиною періоду гами. При цьому, якщо довжина періоду гами перевищує довжину шифротексту, то такий шифр є абсолютно стійким, тобто його не можна розкрити за допомогою статистичної обробки зашифрованого тексту. При шифруванні за допомогою ЕОМ послідовність гами може формуватися за допомогою генератора псевдовипадкових чисел (ПВЧ).

З прикладами використання шифру гамування можна ознайомитись на наступних сайтах:

– https://www.youtube.com/watch?v=SYflmyCSxqw;
– https://sites.google.com/site/anisimovkhv/learning/kripto/labrab/labrab1_3.

ХІД РОБОТИ

1. Адаптувати розроблений у лабораторних роботах №1 та №2 інтерфейс криптографічної системи симетричного шифрування для реалізації шифрування методом гамування.

2. Доповнити систему класів із попередніх лабораторних робіт класами та методами, які необхідні для:

– генерації гами, період якої перевищує довжину вхідного тексту;
– реалізації симетричного шифрування методом гамування.

3. Виконати тестування роботи системи.

4. Додаткові завдання:

– модифікувати розроблену систему, забезпечивши можливість шифрування й розшифрування за допомогою шифроблокноту, як це передбачено у шифрі Вернама.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. У чому полягає суть цього методу шифрування?
2. Різновиди гамування та їх суть.
3. Яким виразом можна описати шифрування і розшифрування для шифру гамування.
4. Двійкове гамування.
5. Ключ шифрування.

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №4

Тема: шифр DES.

Мета: розробити криптосистему на основі шифру DES.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Алгоритм симетричного шифрування DES (Data Encryption Standard) – стандарт симетричного шифрування США, який було розроблено у 1977 році. Згодом цей стандарт шифрування набув міжнародного застосування. Зараз DES вважається ненадійним в основному через малу довжину ключа.

З метою забезпечення більш високого рівня криптостійкості було запропоновано модифікований метод із послідовним трициклічним шифруванням за алгоритмом DES, який отримав назву 3-DES (TripleDES). Криптостійкість методу виявилась значно кращою (про реалізацію успішних атак на 3DES не відомо), проте швидкість шифрування значно зменшилась у порівнянні з DES (приблизно у 3 рази).

На сьогодні алгоритми DES та 3-DES поступово витісняються новітнім алгоритмом шифрування AES (Advanced Encryption Standard), який забезпечує як високий рівень криптостійкості, так і прийнятну швидкість шифрування.

Нові можливості для розробки криптографічних додатків надає бібліотека класів .NET Framework, яка включає класи криптопровайдерів для реалізації симетричного шифрування за чотирма алгоритмами: DES, TripleDES і AES, а також RC2 (який є попередником AES і залишений для забезпечення сумісності із попередніми версіями додатків). Реалізуються вони за допомогою об’єктів двох класів з простору імен System.Security.Cryptography:

– CryptographicServiceProvider – клас, що надає криптопровайдери для кожного з вказаних алгоритмів;

– CryptoStream– клас для роботи з криптографічним потоком.

Застосування цих основних об’єктів вимагає використання об’єкту FileStream з простору імен System.IO. Окрім того, для бітового представлення текстових даних необхідні об’єкти класів UnicodeEncoding (або ASCIIEncoding) з простору імен System.Text.

Шифрування. Порядок шифрування, за їх допомогою, наступний:

1. Створюється необхідний криптопровайдер і задається його ключ і вектор

ініціалізації:

```
DESCryptoServiceProvider cryptic = new DESCryptoServiceProvider();
cryptic.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");
cryptic.IV = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");
cryptic.Mode = CipherMode.CBC;
```

2. Відкривається звичайний файловий потік для запису зашифрованих даних:

```
FileStream stream = new FileStream(@"d:\test.txt",
FileMode.OpenOrCreate,FileAccess.Write)
```

3. Відкритий файловий потік трансформується в криптопотік для запису:

```
CryptoStream crStream = new CryptoStream(fs,
cryptic.CreateEncryptor(),CryptoStreamMode.Write);
```

4. Дані для шифрування перетворюються у бітову послідовність і всі біти (від 0 до data.Length) записуються в криптопотік за допомогою методу Write ():

```
byte[] data = ASCIIEncoding.ASCII.GetBytes("Hello World!");
crStream.Write(data,0,data.Length);
```

5. Використані файловий і криптопотоки закриваються:

```
crStream.Close();
fs.Close();
```

Розшифрування. Порядок розшифрування полягає у наступному:

1. Створюється необхідний криптопровайдер і задаються його ключ і вектор ініціалізації:

```
DESCryptoServiceProvider cryptic = new DESCryptoServiceProvider();
cryptic.Key = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");
cryptic.IV = ASCIIEncoding.ASCII.GetBytes("ABCDEFGH");
cryptic.Mode = CipherMode.CBC;
```

2. Відкривається звичайний файловий потік для читання зашифрованих даних:

```
FileStream stream = new FileStream(@"d:\test.txt",
FileMode.Open,FileAccess.Read)
```

3. Відкритий файловий потік трансформується в криптопотік для читання:

```
CryptoStream crStream = new CryptoStream(stream,
cryptic.CreateDecryptor(),CryptoStreamMode.Read).
```

4. Дані з криптопотоку зчитуються за допомогою об’єкта StreamReader і присвоюються текстовій змінній:

```
StreamReader reader = new StreamReader(crStream);
string data = reader.ReadToEnd();
```

5. Значення текстової змінної виводиться на екран і зчитувач та потік закриваються:

reader.Close(); stream.Close();

З прикладами використання шифру DES можна ознайомитись на наступних сайтах:

– http://surl.li/tmgaz;
– http://surl.li/tmgau;
– http://surl.li/tmgam.

ХІД РОБОТИ

1. Розробити інтерфейс криптографічної системи для шифрування за допомогою DES із використанням усіх можливих режимів.
2. Ознайомитися з описом класів CryptographicServiceProvider і CryptoStream бібліотеки .NET Framework.
3. Реалізувати шифрування DES, використовуючи класи .NET Framework.
4. Виконати тестування роботи системи.
5. Додаткові завдання:

– модифікувати створений програмний код для здійснення шифрування за алгоритмом TripleDES (або AES);

– узагальнити розроблений програмний код, забезпечивши можливість динамічного вибору одного із трьох шифрів – DES, TripleDES, AES.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Алгоритм симетричного шифрування.
2. Чим визначається рівень криптостійкості.
3. Алгоритмом шифрування AES.
4. Які алгоритми застосовують для реалізації симетричного шифрування?
5. У чому перевага модифікованого методу 3-DES над DES?
6. Блочне шифрування. Розмір блоку.
7. Атаки методом повного перебору.

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №5

Тема: шифрування з відкритим ключем на основі задачі рюкзака.

Мета: опанувати методику побудови асиметричних криптосистем.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Першим алгоритмом для узагальненого шифрування з відкритим ключем став алгоритм рюкзака, розроблений Ральфом Меркле і Мартіном Хеллманом. Алгоритм демонструє можливість застосування задачі рюкзака (NP-повної проблеми) в криптографії з відкритими ключами. Задачу рюкзака можна сформулювати так:

Нехай задано множину натуральних чисел $A=(a_1, a_2, ..., an)$ і натуральне число S. Потрібно встановити, чи існує такий набір чисел x_i з (0,1), $i \le n$, для якого $\Sigma a_i x_i = S (1 \le i \le n)$.

Ідея побудови системи шифрування на основі проблеми рюкзака полягає у виділенні деякого підкласу задач про укладання рюкзака, що розв'язуються порівняно легко – задачі «суперзростаючого» рюкзака, і «маскування» задач цього класу за допомогою деякого перетворення параметрів під загальний випадок. Параметри підкласу визначають секретний ключ, а параметри модифікованої задачі – відкритий ключ.

Суперзростаюча послідовність $B=(b_1, b_2, ..., b_n)$ – це послідовність, в якій кожній член більше суми всіх попередніх членів, тобто $b_i > \sum b_j$, де $j<i$. Наприклад, послідовність {1, 3, 6, 13, 27, 52} є суперзростаючою, а {1, 3, 4, 9, 15, 25} – ні.

Розв'язання задачі рюкзака для суперзростаючої послідовності знайти легко, використовуючи такий алгоритм:

Введення: натуральне число $n>1$, натуральне число S, суперзростаюча послідовність натуральних чисел $B=(b_1, b_2, ..., b_n)$.

Виведення: набір чисел xi з (0,1), $i \le n$, для якого $\Sigma a_i x_i = S (1 \le i \le n)$.

Крок 1. Покласти $i=n$.

Крок 2. Порівняти S з найбільшим числом послідовності b_i: якщо $S<b_i$, то $x_i=0$, в іншому випадку $x_i=1$.

Крок 3. Зменшити S на b_i, якщо $x_i=1$.

Крок 4. Покласти $i=n-1$.

Крок 5. Якщо $i>1$, перейти до кроку 2, в іншому випадку повернути набір чисел x_i.

Не суперзростаючі, або нормальні, рюкзаки представляють собою важку NP-проблему – швидкого алгоритму для них не знайдено. Алгоритм Меркле-Хеллмана заснований на цій властивості.

В якості закритого ключа вибирається суперзростаюча послідовність $B=(b_1, b_2, ..., b_n)$ та натуральні числа $m>\Sigma b_i$, і $t \equiv 1 (\mathrm{mod}\ m)$. За ними будується послідовність нормального рюкзака $A=(a_1, a_2, ..., a_n)$ за наступним алгоритмом:

Введення: натуральне число $n>1$, суперзростаюча послідовність

натуральних чисел $B=(b_1, b_2, ..., b_n)$, натуральні числа $m> \Sigma b_i$, і $t\equiv1(\text{mod } m)$.

Виведення: $A=(a_1, a_2, ..., a_n)$.

Крок 1. Покласти i=1.

Крок 2. Знайти $a_i=b_i\times t(\text{mod } m)$.

Крок 3. Покласти i=i+1.

Крок 4. Якщо i>n, повернути A, в іншому випадку перейти до кроку 2.

Відкритий ключ $A=(a_1, a_2, ..., a_n)$ використовується для шифрування за таким алгоритмом:

Введення: натуральне число n>1, послідовність натуральних чисел $A=(a_1, a_2, ..., a_n)$, вхідне повідомлення p.

Виведення: шифротекст C.

Крок 1. Представити p у вигляді бінарної послідовності.

Крок 2. Розбити отриману бінарну послідовність на n-розрядні блоки $p_i=p_{i1}p_{i2}, \ldots, p_{in}$.

Крок 3. Зашифрувати кожний блок за допомогою перетворення $C_i=\Sigma p_{ij}\times a_j$, де j=1...n.

Крок 4. Отримати шифротекст $C=(C_1; C_2; \ldots; C_i)$.

Зашифроване повідомлення може розшифрувати власник закритого ключа, скористувавшись наступним алгоритмом:

Введення: натуральне число n>1, супер зростаюча послідовність натуральних чисел $B=(b_1, b_2, ..., b_n)$, натуральні числа $m>\Sigma b_i$, і $t\equiv1(\text{mod } m)$, шифротекст $C=(C_1; C_2; \ldots; C_i)$.

Виведення: відкрите повідомлення p.

Крок 1. Знайти таке дійсне t^{-1}, якщо $tt^{-1}\equiv1(\text{mod } m)$.

Крок 2. Для кожного блоку шифротексту обчислити Ci/≡t-1Ci(mod m).

В принципі вирішення задачі рюкзака завжди може бути знайдено повним перебором підмножин A і перевіркою, яка з їх сум дорівнює S. Але при великих n доведеться перебрати 2^n варіантів. Навіть для n=300 пошук серед 2300 підмножин не піддається обробці.

З прикладами використання шифру за алгоритмом рюкзака можна ознайомитись на таких сайтах:

– http://surl.li/tnsdg;
– http://surl.li/tnsfd.

ХІД РОБОТИ

1. Відшукайте в Internet-ресурсах будь-який приклад із використанням «рюкзачного» алгоритму та опрацюйте його.

2. Розробити інтерфейс криптографічної системи для шифрування із

використанням задачі рюкзака, передбачивши окремий діалог для формування відкритого ключа.

3. Розробити методи, які б забезпечували:

– генерацію пари «відкритий-закритий» ключ;

– шифрування із використанням відкритого ключа;

– розшифрування із використанням закритого ключа (при цьому значення t^{-1} вважати відомим).

4. Перевірити правильність роботи системи на основі використання даних із знайденого в Internet-ресурсах прикладу.

5. Додаткові завдання:

– ознайомитись із можливостями онлайн калькулятора для знаходження взаємно обернених чисел, використайте його для t^{-1} за відомими t і перевірити правильність функціонування системи для загального випадку;

– ознайомитись із розширеним алгоритмом Евкліда для знаходження взаємно обернених чисел і модифікувати створений програмний код, додавши метод із реалізацією цього алгоритму і використання його для знаходження t^{-1} за відомими t і m.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. У чому полягає суть задачі рюкзака.
2. Секретний та відкритий ключ.
3. Суперзростаюча послідовність.
4. Алгоритм Меркле-Хеллмана.
5. Алгоритми відкритого і закритого ключів.

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №6

Тема: шифрування з відкритим ключем на основі алгоритму RSA.

Мета: ознайомитись із використанням криптопровайдерів .Net для побудови асиметричної криптосистеми.

Завдання: опрацювати теоретичний матеріал, протестувати та дослідити розроблену криптосистему шифрування.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Шифр RSA отримав назву на честь його розробників Рона Ріверса, Аді Шаміра та Леонарда Адлемана (Leonard Adleman). В RSA системі використовуються наступні факти з теорії чисел:

1) Задача перевірки числа на простоту є порівняно простою.

2) Задача розкладання числа n=p×q, де p і q – прості числа, на множники є дуже складною задачею, якщо ми знаємо тільки n, а p і q – великі числа (задача факторизації).

Основні повідомлення між сторонами B і A в протоколі RSA представляються наступною діаграмою:

A↔B: N=PQ, де P і Q – прості;

B: f=(P-1)(Q-1); d<f, взаємно просте з f; cd mod f=1;

B→A: d;

A:m; A→B: $e=m^d \bmod N$

B: y; B→A: $m'=e^c \bmod N$.

Алгоритм гарантує, що $m'=m$. Пара чисел (c, N) є секретним, а (d, N) – публічним ключем сторони B.

На платформі .NET алгоритм RSA реалізується за допомогою об'єктів класу RSACryptoServiceProvider з простору імен System.Security.Cryptography. Генерація відкритого та закритого ключів здійснюється при створенні нового екземпляра класу. Після створення нового екземпляра класу можна отримати інформацію про ключ одним із двох способів:

1) Метод ToXMLString – повертає інформацію про ключ в форматі XML.

2) Метод ExportParameters – повертає структуру RSAParameters, яка містить ключові відомості.

Обидва методи приймають за параметр логічне значення, яке показує:

– false – слід повертати відомості тільки про відкритий ключ;

– true – слід повертати відомості і про відкритий, і про закритий ключі.

Ініціалізація класу RSACryptoServiceProvider може бути здійснена також двома шляхами:

1) Метод FromXmlString – використовує дані ключа з рядка XML.

2) Vtnjl ImportParameters – dbrjhbcnjdeє lfyi cnhernehb RSAParameters/

Асиметричні закриті ключі ніколи не повинні зберігатися в роздрукованому вигляді або у вигляді простого тексту на локальному комп'ютері. Якщо необхідно зберігати закритий ключ, то необхідно використовувати для цього контейнер ключа. Контейнер ключа представляє собою екземпляр класу CspParameters (з простору імен System.Security.Cryptography).

При цьому в полі CspParameters.KeyContainerName задається ім'я контейнера.

Розшифрування. Порядок розшифрування за допомогою об'єктів класу RSACryptoServiceProvider наступний:

1) Створюється контейнер для збереження ключів:

```
CspParameters cp = new CspParameters();
cp.KeyContainerName = "Key Name";
```

2) Створюється екземпляр криптопровайдера з розміщенням ключів у контейнері:

```
RSACryptoServiceProvider rsa = new RSACryptoServiceProvider(cp)
```

3) Публічний ключ експортується для передачі іншій стороні:

```
string pubKey = rsa.ToXmlString(false);
Console.WriteLine("Public Key: \n {0}", pubKey);
```

4) Після отримання байтових даних byte[] EncryptBytes, зашифрованих за допомогою публічного ключа, здійснюється їх розшифрування за допомогою закритого ключа:

```
byte[] DecryptBytes = rsa.Decrypt(EncryptBytes, false);
string decryptStr = Encoding.Unicode.GetString(DecryptBytes);
//string decryptStr =BitConverter.ToString(DecryptBytes);
Console.WriteLine("Decripted string: \n {0}", decryptStr);
```

Шифрування. Порядок шифрування полягає у наступному:

1) Створюється екземпляр криптопровайдера:

```
RSACryptoServiceProvider rsa1 = new RSACryptoServiceProvider()
```

2) Імпортується публічний ключ:

```
rsa1.FromXmlString(pubKey);
```

3) Текст повідомлення перетворюється у байтову послідовність і зашифровується публічним ключем:

```
string dataToEncrypt = "Data to encrypt";
byte[] byteToEncript = Encoding.Unicode.GetBytes(dataToEncrypt);
byte[] EncryptBytes = rsa1.Encrypt(byteToEncript, false);
```

4) Зашифрована байтова послідовність відправляється стороні, яка має для розшифрування відповідний закритий ключ.

З прикладами використання шифру за алгоритмом RSA можна ознайомитись на наступних сайтах:

- http://surl.li/cgnzj;
- https://dou.ua/forums/topic/43026/;
- http://surl.li/tqijv.

ХІД РОБОТИ

1. Відшукайте в Internet-ресурсах будь-який приклад із використанням алгоритму RSA та опрацюйте його.

2. Розробити інтерфейс криптографічної системи для шифрування з використанням RSA, передбачивши окремий діалог для формування відкритого ключа.

3. Розробити методи, які б забезпечували:

– генерацію пари «відкритий-закритий» ключ;

– шифрування із використанням відкритого ключа;

– розшифрування із використанням закритого ключа.

4. Перевірити правильність роботи системи на основі використання даних із знайденого в Internet-ресурсах прикладу.

5. Додаткові завдання:

– ознайомитись із можливостями онлайн калькулятора для розкладання числа на прості множники і скористайтесь ним для проведення атаки на шифр RSA;

– визначте область значень параметрів шифру RSA, за яких така атака є реальною.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Шифр RSA.
2. Які параметри теорії чисел використовуються в RSA системі?
3. Які способи дозволяють отримати інформацію про ключ?
4. Асиметричні закриті ключі.
5. Контейнер ключа.
6. Який порядок дій при шифруванні/розшифруванні?

Рекомендована література: [1; 2; 4-6; 8-13].

ЛАБОРАТОРНА РОБОТА №7

Тема: дослідження звукоізоляційних властивостей матеріалів.

Мета: дослідити можливості забезпечення пасивних засобів захисту від акустичного каналу перехоплення інформації.

Завдання: опрацювати теоретичний матеріал, виміряти загальний рівень шуму в звукоізолюючій камері та виконати необхідні розрахунки.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Звукоізоляція – це властивість конструкцій затримувати частину енергії звукових хвиль, які потрапляють на них, тобто зниження рівня шуму, який надходить у приміщення зовні. Коефіцієнт звукоізоляції визначають із співвідношення інтенсивності падаючих хвиль до хвиль, які пройшли через

загороджувальну поверхню. Інтенсивність звуку – це кількість енергії, яка проходить через одиницю площі за одну секунду, та направлена перпендикулярно до розповсюдження хвиль (Вт/м^2).

Коефіцієнт звукоізоляції розраховується за виразом (7.1):

$$\rho = \frac{I_{пд}}{I_{пр}}, \tag{7.1}$$

де $I_{пд}$ та $I_{пр}$ – інтенсивність звуку падаючої та пройденої хвилі.

При цьому, інтенсивність звуку, в загальному, являє собою (7.2):

$$I = \frac{\Delta p^2}{2U_w \rho}, \tag{7.2}$$

де Δp^2 – зміна звукового тиску;

ρ – густина матеріалу, через який проходить хвиля;

U_w – швидкість звуку.

Шум – це неперіодичне звукове коливання різної інтенсивності та частоти. Повітряний шум – це коливання, середовищем розповсюдження яких є повітряні потоки.

Структурний шум – це механічні коливання, які розповсюджуються у твердому тілі із частотою від 16 до 20 кГц (механічні коливання стін, перекриття та трубопроводів). У результаті цієї взаємодії виникають напруження і деформації, які й утворюють структурні коливання.

В порівнянні із повітряним шумом, для розповсюдження структурних коливань в приміщеннях та інженерних конструкціях притаманні наступні особливості:

– швидкість розповсюдження структурних хвиль залежить від частоти;

– відбивання від межі середовища (наприклад, складові елементи стін, кути тощо);

– перетворення типів хвиль (наприклад, із згинів в повздовжні);

– затухання хвиль через відбивання або поглинання (наприклад, перехід енергії в тепло).

Звукопоглинання – це процес поглинання звукової енергії в теплову під час розповсюдження звуку в середовищі або під час його потрапляння на межу двох середовищ «повітря/загороджувальна поверхня». Звукопоглинання характеризується коефіцієнтом звукопоглинання. Під час створення звукопоглинаючого об’єкта необхідно зрозуміти яким чином звукова хвиля буде

розповсюджуватись у ньому. Згенеровані джерелом звуку звукові хвилі діють на поверхню, після чого одна їх частина відбивається, а інша, у вигляді еха, розповсюджується у цій поверхні (конструкції) зі швидкість 4200-5300 м/с. Процес поступового зменшення інтенсивності звука, який був відбитим від перешкоди звукової хвилі, до повного його затухання називають реверберацією. Візуально такий процес подано на рисунку 7.1.

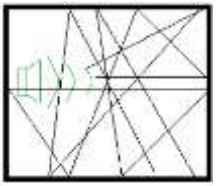

Рисунок 7.1 – Реверберація

Ехосигнал являє собою відбиту від перешкоди звукову хвилю. Явище реверберації складається із суперпозиції різних ехосигналів від одного джерела звуку. Зменшення часу реверберації в приміщенні за допомогою звукопоглинаючих матеріалів призводить до зменшення шуму. Час реверберації прийнято розраховувати за виразом (7.3):

$$T = \frac{0{,}164V}{A}, \tag{7.3}$$

$$A = a_1S_1 + a_2S_2 + ... + a_iS_i, \tag{7.4}$$

де T – час реверберації;

A – загальний фон звукопоглинання;

a – коефіцієнт звукопоглинання;

V – об'єм приміщення;

S – площа поверхні.

Коефіцієнт звукопоглинання визначається з виразу (7.1). Оскільки інтенсивність звуку вимірюється в Вт/м^2, то спочатку необхідно перевести за виразом (7.5) децибели та вати:

$$I = 10 \cdot \lg\left(\frac{P}{P_0}\right), \tag{7.5}$$

де P – звуковий тиск;

P_0 – граничне значення звукового тиску.

ХІД РОБОТИ

1. Скласти лабораторну установку для аналізу потенційного каналу витоку інформації за структурною схемою, яка подана на рисунку 7.2.

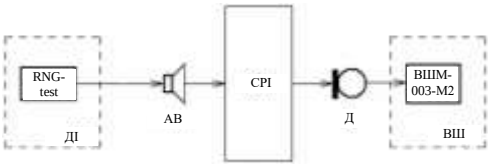

Рисунок 7.2 – Структурна схема установки:
ДІ – джерело інформації; АВ – акустичний випромінювач; СРІ – середовище розповсюдження інформації; Д – давач (датчик); ВШ – прилад для вимірювання шуму

Акустичний випромінювач з'єднати із джерелом гармонійних сигналів RNG-test. Після цього розташувати ДІ в шумоізоляційній камері СРІ.

Передпідсилювач мікрофонний ВНП-101 з капсулем мікрофонним конденсаторним М-101 встановити перед шумоізоляційною камерою на відстані 1 м. Передпідсилювач мікрофонний з'єднати із приладом для вимірювання шуму ВШМ-003-М2.

2. Виміряти загальний рівень шуму (без встановлення в звукоізолюючій камері звукоізолюючих матеріалів).

3. Виміряти рівень шуму в звукоізолюючій камері після розташування в одній із її стінок досліджуваного матеріалу (картон, пінопласт). Результати звести до таблиці 7.1.

Таблиця 7.1 – Результати дослідження

Назва матеріалу	Частота, Гц				
	250	500	1000	2000	4000
Без матеріалу, Вт					
Ізолюючий матеріал 1, Вт					
Ізолюючий матеріал 2, Вт					

4. Перевести значення звукового тиску у вати за допомогою виразу (7.5).

5. Встановити, виходячи з виразу (7.1), значення коефіцієнта звукоізоляції. Результати розрахунків звести до таблиці 7.2.

Таблиця 7.2 – Розрахункові значення коефіцієнта звукоізоляції

Назва матеріалу	Частота, Гц				
	250	500	1000	2000	4000
Без матеріалу, Вт					
Ізолюючий матеріал 1, Вт					
Ізолюючий матеріал 2, Вт					

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Шумоізоляція.
2. Яка різниця між звукопоглинанням та звукоізоляцією?
3. Назвіть найбільш розповсюджені пористі звукопоглинаючі матеріали.
4. Назвіть найбільш розповсюджені однорідні звукопоглинаючі матеріали.
5. Резонансний поглинач.

Рекомендована література: [2; 5; 7; 11; 14].

ЛАБОРАТОРНА РОБОТА №8

Тема: атестація приміщення за вимогами безпеки інформації.

Мета: опанувати методику атестації приміщення відповідно до вимог безпеки інформації.

Завдання: опрацювати теоретичний матеріал, сформувати план-схему досліджувального приміщення та передбачити заходи для проведення візуального огляду з метою виявлення закладних пристроїв.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Враховуючи досвід організації спеціальних досліджень, для скорочення часу робіт які проводяться під час атестації приміщень вимогам безпеки інформації Замовник перед проведенням підготовчого етапу має надати такі вихідні дані:

1. Атрибути об’єкта – повна адреса Замовника, повне найменування об’єкта, а також його розміщення (поверх, № або назва приміщення).

2. Контрольована зона (КЗ) – реквізити документа, який встановлює КЗ. Надається планування, яке визначає розміщення об’єкта на генплані, його місце розташування із зазначенням назви вулиць, скверів тощо. Мінімальна відстань від об’єкта до межі КЗ).

3. Категорія об’єкта.

4. Приміщення, які межують з об’єктом (спереду, ззаду, праворуч, ліворуч, знизу, зверху).

5. Огороджувальні конструкції (спереду, ззаду, праворуч, ліворуч, знизу, зверху). Необхідно за кожним напрямком вказати вид матеріалу конструкції та його товщину. Якщо конструкція складна, тобто виконання в кілька шарів, необхідно перерахувати всі шари із зазначенням товщини кожного. Зазначити наявність наскрізних щілин і пустот в огороджувальних конструкціях.

6. Наявність фальшпідлоги і фальшстелі (із зазначенням типу, матеріалу, товщини й відстані від перекриття до фальшпідлоги/стелі).

7. Опис дверей приміщення (матеріал, розміри, подвійні/одинарні, одностулкові/двостулкові, наявність порога і його висота).

8. Опис вікон приміщення (матеріал, розміри, подвійні/одинарні, товщина скління). Куди виходять вікна – внутрішній двір, вулиця тощо.

9. Система опалення. Де розташований тепловий пункт. Як побудована система опалення (тип радіаторів опалення, як здійснюється подача теплоносія, кількість радіаторів, кількість стояків опалення в приміщенні).

10. Система водопостачання (опис аналогічний системі опалення).

11. Система вентиляції (кількість вентиляційних каналів, перетин коробів та їх місцезнаходження із зазначенням найближчих виходів в інші приміщення).

12. Опис застосовуваних засобів захисту (марка, вид апаратури захисту, місця встановлення датчиків тощо).

На підготовчому етапі проводять якісну оцінку вібро- і звукоізоляції приміщення з метою визначення найімовірніших розвідувально-небезпечних напрямків. Аналізують архітектурно-планувальні рішення приміщення, конструктивні особливості його огороджувальних конструкцій (стін, перекриттів, дверей, вікон) та інженерно-технічних систем. Обстежуються комунікації трубопроводів різних систем життєзабезпечення, виявляються неоднорідності в огороджувальних конструкціях, обстежуються конструктивні особливості елементів оздоблення. Уточнюються просторові співвідношення огороджувальних конструкцій приміщення та елементів технічних систем відносно встановленої межі контрольованої зони і відносно прилеглих до контрольованої зони будівель, споруд тощо.

Оцінюється (або уточнюється) ступінь секретності мовленнєвої інформації (категорії об’єкта захисту) і визначається необхідне значення нормованого показника протидії акустичній мовленнєвій розвідці, на відповідність якому необхідно проводити інструментальний контроль.

Уточнюються умови мовленнєвої діяльності в контрольованому приміщенні. Проводиться слуховий (якісний) контроль звукоізоляції огороджувальних конструкцій шляхом прослуховування сигналів, що формуються в контрольованому приміщенні. Як такі сигнали рекомендується використовувати природну мову, записану, наприклад, на магнітофон.

Приклад вихідних даних для складання плану пошуку. Зауважимо, що такі дані виконуються самостійно шляхом огляду виділеного приміщення та прилеглої території.

Представник ТзОВ «Відеонагляд», як представник Замовника, представив такі вихідні дані на досліджуване приміщення:

1. Атрибути об’єкта – ТзОВ «Відеонагляд», м. Луцьк, вул. Будівельників, будинок №5, розташоване на першому поверсі 3-х поверхової будівлі. На 2-му і 3-му поверхах розташовані сторонні організації. Є загальна територія, що охороняється. Допуск сторонніх осіб і автомобілів тільки за згодою керівника ТзОВ «Відеонагляд» й керівників сторонніх організацій. Усі співробітники ТзОВ «Відеонагляд» мають допуск не нижче третього. Сторонні організації з держтаємницею не працюють. У ТзОВ «Відеонагляд» є одне виділене приміщення (ВП) – кабінет керівника. Планується його атестація як виділеного приміщення – приміщення для переговорів.

2. Контрольована зона (КЗ) об’єкта проходить по огороджувальних конструкціях третього поверху, за винятком сходів на верхні поверхи. Досліджувана ВП – переговорна – межує з КЗ по одній стіні, на якій розташовані одне вікно і двері, та по стелі. Засоби звукопідсилення в переговорній відсутні. Джерело мови не локалізоване.

3. Приміщенню планується встановити 2-гу категорію.

4. Приміщення, які межують (спереду/ззаду, праворуч/ліворуч, знизу/зверху).

5. Огороджувальні конструкції:

– стіни 1 і 2 виконано із цегли – товщина 2,5 цегли; внутрішня штукатурка товщиною 1 см;

– бічні стіни 3 і 4 виконані з цегли – товщина 1 цегла; всередині й зовні штукатурка товщиною 1 см;

– підлога й стеля виконані із стандартних бетонних плит перекриття товщиною 30 см; підвалу немає; наскрізних щілин і пустот не виявлено; підлога дерев’яна на лагах, покрита лінолеумом;

– фальшстелі немає.

6. Двері подвійні з тамбуром. Ширина тамбура - 0,5 м. По периметру кожних дверей прокладено ущільнювач. Двері важкі дерев’яні. Дверні коробки відокремлені одна від одної та від стіни гумовими ущільнювачами. Двері виходять на кордон КЗ.

7. Вікно пластикове у спеціальному виконанні. Рама вікна відокремлена від стіни гумовими прокладками. Вікно межує з КЗ.

8. У приміщенні є одна батарея опалення. Труби системи опалення виконані з металопластику. Введення труби системи опалення здійснено з другого поверху, вихід труби йде під підлогу. Тепловий пункт розміщено за межами КЗ. Таким чином, система опалення має вихід за межі КЗ.

9. Система вентиляції виконана у вигляді вентиляційних коробів і має найближчий вихід до загального коридору першого поверху, а потім виходить на

другий і третій поверх (за планом).

10. На елементах огороджувальних конструкцій та інженерних комунікацій є засоби активного захисту.

Методика проведення огляду приміщень. Усю процедуру пошуку пристроїв негласного знімання інформації доцільно розділити на декілька етапів:

– підготовчий етап;

– фізичний пошук та візуальний огляд;

– виявлення радіо-закладних пристроїв;

– виявлення технічних засобів з передачею інформації струмоведучими лініями;

– виявлення закладних пристроїв з передачею інформації ІЧ-каналом;

– перевірка наявності акустичних каналів витоку інформації.

Підготовчий етап. Цей етап призначений для визначення глибини пошуку, а також формування переліку йпорядку проведених заходів. Він містить такі елементи:

1. Оцінка можливого рівня використовуваних технічних засобів (обсяг проведених заходів істотно залежить від того, в чиїх інтересах їх проводять).

2. Аналіз ступеня небезпеки, який виходить від своїх співробітників і представників сусідніх організацій (дієвим способом перевірки є організація контрольованого витоку інформації).

3. Оцінка можливості доступу сторонніх осіб у приміщення.

4. Вивчення історії об'єкта, в якому планується проводити пошукові заходи (оцінюється можливість встановлення закладок як під час будівництва, так і залишення їх у спадок від попередніх мешканців).

5. Визначення рівня підтримуваної безпеки відповідно до економічних можливостей і ступеня бажання замовника, а також фактичної необхідності.

6. Вироблення плану дій, який має відповідати таким умовам:

– час пошуку має припадати на робочі години, коли ЗП активізовані;

– мають бути створені умови, які б спровокували до дії можливо впроваджені «жучки», оскільки в них можуть бути використані як схеми VOX, що вмикають пристрої тільки за певного рівня акустичного сигналу, так і системи дистанційного керування (проведення фіктивних, але правдоподібних ділових перемовин – гарний привід, щоб спонукати протилежну сторону активізувати свої пристрої);

– має бути забезпечено скритність заходів, що проводяться, – якщо є потреба ведення своєї «контррозвідувальної» гри, то варто пам'ятати, що розмови з колегами та замовлення, прихід, розгортання апаратури, характерний

шум пошуку розкривають зміст та результат заходів, що проводяться;

– неочікуваність – пошук варто проводити у формі негласного знімання інформації, а також у формі негласного знімання інформації.

Фізичний пошук й візуальний огляд. Фізичний пошук та візуальний огляд є важливим елементом виявлення засобів негласного знімання інформації, особливо таких, як дротові та волоконно-оптичні мікрофони, пасивні й напівактивні радіозакладні пристрої, дистанційно керовані пристрої, які «очікують», та інші технічні засоби, які неможливо виявити за допомогою звичайної апаратури.

Варто зауважити, що будь-який фізичний пошук є базою для будь-якої пошукової методики. Проведення пошукових заходів слід починати з підготовки приміщення, що підлягає перевірці:

1. Необхідно закрити всі вікна й ролети для виключення візуального контакту.

2. Увімкнути світло і всі звичайні офісні пристрої, характерні для цього приміщення.

3. Увімкнути джерело «відомого звуку» (тестового акустичного сигналу) у центрі зони контролю. Під час пошуку воно виконуватиме важливі функції: маскуватиме більшість шумів, які формуються під час фізичного пошуку; працюватиме як джерело для звукового зворотного зв'язку, необхідного для виявлення радіо-мікрофонів; активізуватиме пристрої, оснащені системою VOX. Джерело «відомого звуку» не повинне насторожувати протилежну сторону, отже, це може бути будь-який плейєр. Слід пам'ятати, що найкращі результати досягаються при використанні апаратури середніх розмірів. Це пояснюється оптимальними розмірами гучномовця. Виберіть найбільш доречний у даній ситуації запис, чи то музика, чи то бізнес-семінар, чи то курс самонавчання. Підберіть відповідну тривалість, оскільки якісний пошук може зайняти багато годин.

4. За межами зони контролю (у незахищеній кімнаті/зоні) якомога безшумно розгорніть вашу апаратуру. Незахищена зона – це місце, яке не викликає інтересу у протилежної сторони і не контролюється нею, тому ваші дії залишаться прихованими.

5. Встановіть звичайний рівень радіовипромінювання навколишнього середовища перед пошуком у зоні контролю.

Основні процедури пошуку. Візуально, а також за допомогою засобів відеоспостереження та металодетекторів, обстежте всі предмети в зоні контролю, розміри яких достатньо великі для того, щоб можна було розмістити в

них технічні засоби негласного знімання інформації. Ретельно огляньте й розкрийте, у разі потреби, всі настільні прилади, рами картин, телефони, квіткові горщики, книжки, пристрої, що живляться від мережі (комп'ютери, ксерокси, радіоприймачі тощо).

Для пошуку прихованої проводки обстежте плінтуси і підніміть килимові покриття. Ретельно огляньте стельові панелі, а також усі пристрої, що містять мікрофони, магнітофони та камери.

З особливою ретельністю обстежте місця, де ведуться найважливіші переговори (зазвичай це стіл із телефоном).

Варто пам'ятати, що більшість нелегальних пристроїв розташовуються в радіусі 7 м від цього місця для забезпечення найкращої чутності та (або) видимості.

Якщо ви при цьому використовуєте металодетектор, то ретельно виконуйте вимоги його інструкції на експлуатацію.

Особливо слід звернути увагу на перевірку телефонних ліній, мереж пожежної та охоронної сигналізації. Слід обов'язково розібрати телефонний апарат, розетки і датчики та шукати деталі, несхожі на звичайні, з різнокольоровими дротами й поспішним або неакуратним встановленням. Потім огляньте лінію від апарата (датчика) до стіни та, видаливши стінну панель, перевірте, чи немає за нею нестандартних деталей.

Проведіть фізичний пошук у комутаційних панелях і комунікаційних каналах, у разі потреби використовуйте ендоскопічні та портативні телевізійні засоби відеоспостереження. Перевірте місця входу/виходу проводів всередині та зовні будівлі.

З метою полегшення подальших пошукових заходів після завершення всіх робіт потай помітьте шурупи на стінних панелях, мережевих розетках, телефонних корпусах та інших місцях, куди можуть бути встановлені закладки. Тоді при проведенні повторних перевірок видимі в ультрафіолетових променях мітки покажуть порушення цілісності раніше обстеженого об'єкта, якщо воно мало місце, а відповідні записи у вашому журналі перевірок допоможуть зорієнтуватися в майбутній роботі. Для контролю змін у навколишніх пристроях дуже зручні ультрафіолетові маркери.

Під час проведення пошуку закладних пристроїв в автомобілі ретельно огляньте не тільки салон, а й раму автомобіля, багажник тощо, уважно перевірте ланцюги, які мають вихід на автомобільну антену. Зазначимо, що під час проведення цих операцій оглядові портативні телевізійні системи також можуть виявитися дуже корисними.

ХІД РОБОТИ

1. Скласти або отримати документацію на контрольоване приміщення, вивчити її, визначити можливі розвідувально-небезпечні напрямки та можливі види розвідки.
2. Подати план-схему досліджуваного приміщення.
3. Спираючись на наведену у роботі методику скласти план проведення візуального огляду приміщення та виявити об'єкти, які потребують під час обстеження використання наявних засобів відеоспостереження.
4. За результатами виконаної роботи зробити висновок та підготувати звіт.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Які вихідні дані необхідні для складення плану пошуку?
2. Методика проведення огляду приміщення.
3. Основні процедури пошуку.

Рекомендована література: [2; 5; 7; 11; 14].

ЛАБОРАТОРНА РОБОТА №9

Тема: виявлення витоку інформації технічними каналами за допомогою багатофункціональних пошукових приладів.

Мета: опанувати методику проведення заходів щодо виявлення та локалізація спеціальних технічних засобів таємного добування інформації, виявлення природних та штучно-створених каналів витоку інформації багатофункціональними пошуковими приладами.

Завдання: опрацювати теоретичний матеріал, провести пошук та ідентифікацію радіозакладного пристрою використовуючи запропоновані детектори.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Під витоком інформації необхідно розуміти несанкціонований процес перенесення інформації від джерела до зловмисника.

Витік інформації можливий шляхом її розголошення людьми, втрата ними носіїв з інформацією, перенесення інформації за допомогою полів, потоків елементарних частинок, речовини в газоподібному, рідкому або твердому вигляді.

Способи доступу до конфіденційної інформації можна поділити на дві групи у залежності від способів доступу її органів добування – агентів або технічних засобів – до джерел інформації та забезпечення розвідувального

контакту з ними.

Розвідувальний контакт між зловмисником або його технічним засобом та джерелом інформації передбачає встановлення фізичного контакту між зловмисником (технічний засіб) і носієм інформації. Фізичний контакт передбачає, що зловмисник має можливість взяти носій з інформацією в руки з метою його викрадення, копіювання, знищення або модернізації або за допомогою своїх рецепторів та використовуваних технічних засобів добування – зняти з носія інформацію дистанційно.

Дистанційне добування інформації передбачає знімання її з носія, що поширюється за межі області фізичного контакту зловмисника з джерелом інформації.

Часто розглядають варіант, коли інформація знімається за межами контрольованої зони, але й можливими є і інші варіанти. Дистанційне добування інформації можливе в результаті спостереження, підслуховування, перехоплення, збір носіїв інформації у вигляді матеріальних тіл – браковані вузли, деталі, демаскуючі речовини та поля за межами організації чи контрольованої зони, наприклад – акустичних, електричних, магнітних і електромагнітних полів, в тому числі в оптичному діапазоні; електричний струм, який поширюється у провідниках електроживлення, телефонна мережа, радіотрансляція, охоронна і пожежна сигналізація.

Витік інформації технічними каналами має ряд особливостей, які необхідно враховувати:

– витік інформації може відбуватися тільки при попаданні її до зацікавленого в ній несанкціонованого одержувача;

– під час витоку інформації відбувається її тиражування, яке не змінює характеристики носія інформації;

– ціна інформації при її витоку зменшується при тиражуванні;

– витік інформації, як правило, виявляється через деякий час, за наслідками, коли заходи щодо забезпечення її безпеки можуть виявитися неефективними.

Фізичний шлях перенесення інформації від її джерела до несанкціонованого одержувача (зловмисника) називається каналом витоку. Канал, в якому здійснюється несанкціонований процес перенесення інформації з використанням технічних засобів, називають технічним каналом витоку інформації.

Характеристики технічних каналів витоку інформації. Для передачі інформації носіями у вигляді полів та мікрочастинок по будь-якому технічному каналові сам канал повинен містити три основних елементи: джерело сигналу,

середовище поширення носія і приймач.

Узагальнена типова структура каналу передачі інформації наведена на рисунку 9.1.

Рисунок 9.1 – Типова структура каналу передачі інформації

На вхід каналу надходить інформація у вигляді первинного сигналу. Первинний сигнал являє собою носій з інформацією від її джерела або з виходом попереднього каналу. У якості джерела сигналу можуть виступати:

– об’єкт спостереження, який відображає електромагнітні та акустичні хвилі;

– об’єкт спостереження, який випромінює власні (теплові) електромагнітні хвилі в оптичному і радіодіапазоні;

– передавач функціонального каналу зв’язку;

– закладний пристрій;

– джерело небезпечного сигналу;

– джерело акустичних хвиль, модульованих інформацією.

Так як інформація від джерела надходить на вхід каналу на мові джерела (у вигляді тексту, символів, знаків, звуків, сигналів тощо), то передавач перетворює ці форми подання інформації у форму, що забезпечує запис її на носій інформації, відповідно середовищу поширення. У загальному випадку він виконує наступні функції:

– створює (генерує) поля (акустичне, електромагнітне) або електричний струм, які переносять інформацію;

– проводить запис інформації на носій (модуляцію інформаційних параметрів носія);

– підсилює потужність сигналу (носія з інформацією);

– забезпечує передачу (випромінювання) сигналу в середу поширення в заданому секторі простору.

– Середовище поширення носія – частина простору, в якому переміщується носій. Воно характеризується набором фізичних параметрів, що

визначають умови переміщення носія з інформацією. Основними параметрами, які доцільно враховувати під час опису середовища поширення, виступають:

– фізичні перешкоди для суб'єктів і матеріальних тіл;

– ступінь ослаблення (або пропускання енергії) сигналу на одиницю довжини;

– частотна характеристика (нерівномірність ослаблення частотних складових спектра сигналу);

– вид і потужність перешкод для сигналу.

Приймач виконує функції, зворотні функції передавача. Він здійснює:

– вибір (селекція) носія з необхідною одержувачу інформацією;

– посилення прийнятого сигналу до значень, що забезпечує знімання інформації;

– знімання інформації з носія (демодуляція, декодування);

– перетворення інформації в форму сигналу, доступного одержувачу (людина, технічний пристрій) і посилення сигналів до значень, необхідних для безпомилкового їх сприйняття.

Канал витоку інформації відрізняється від функціонального каналу передачі одержувачем інформації. Якщо одержувач санкціонований, то канал функціональний, в іншому випадку – канал витоку.

Класифікація технічних каналів витоку інформації. Основною класифікаційною ознакою технічних каналів витоку інформації є фізична природа носія. За цією ознакою вони поділяються:

– візуально-оптичні;
– акустичні;
– електричні;
– радіотехнічні;
– матеріально-мовленевий.

Носієм інформації в оптичному каналі є електромагнітне поле в діапазоні від 0,46 до 0,76 мкм (видиме світло) та від 0,76 до 13 мкм (інфрачервоне випромінювання).

У радіоелектронному каналі витоку інформації в якості носіїв використовуються електричні, магнітні та електромагнітні поля в радіодіапазоні, а також електричний струм (потік електронів), що поширюється по металевих провідниках. Діапазон коливань носія цього виду надзвичайно великий: від звукового діапазону до десятків ГГц.

Відповідно радіоелектронний канал доцільно розділити на 2 підвиди: електромагнітний, носіями інформації в якому є електричне, магнітне і

електромагнітне поля, та електричний канал, носій інформації в якому виступає електричний струм.

Носіями інформації в акустичному каналі є механічні пружні акустичні хвилі в інфразвуковому (менші за 16 Гц), звуковому (від 16 Гц до 20 кГц) і ультразвуковому (понад 20 кГц) діапазоні частоти, що поширюється в атмосфері, воді та твердому середовищі.

У матеріально-мовленевому каналі витік інформації проводиться шляхом несанкціонованого поширення за межі організації речових носіїв з інформацією, яка захищається (наприклад, чернетки документів і використана копіювальна стрічка та папір, забраковані деталі і вузли, демаскуючі речовини, брухт, технологічні відходи).

Кожен із технічних каналів має свої особливості, які необхідно знати й враховувати для забезпечення ефективного захисту інформації.

За своєю інформативністю канали витоку діляться на інформативні та неінформативні. Інформативність каналу оцінюється цінністю інформації, яка передається по каналу.

За часом прояву канали діляться на постійні, періодичні та епізодичні. У постійному каналі витік інформації носить досить регулярний характер. Так, наявність в приміщені джерела небезпечного сигналу може передбачати передачу з кабінету мовленевої інформації до моменту виявлення цього джерела. Періодичний канал витоку може виникнути за умови, наприклад, розміщення у дворі не прикритої продукції, демаскуючі ознаки про яку складають таємницю, під час прольотів розвідувальних космічних апаратів. До епізодичних каналів належать канали, витік інформація в яких має випадковий разовий характер.

Канал витоку інформації, який складається із передавача, середовища поширення і приймача, є одноканальним. Однак можливі варіанти, коли витік інформації відбувається більш складним шляхом – за декількома послідовними або паралельними каналами.

Радіозакладні пристрої. Для виявлення радіозакладок застосовують індикатори електромагнітного поля, частотоміри, нелінійні локатори, рентгенотелевізійну апаратуру та спеціальні скануючі приймачі. За їх допомогою здійснють пошук та фіксацію робочих частот радіозакладок, а також визначається їх місцезнаходження.

Якщо радіозакладки вимкнені у момент пошуку і не випромінюють сигнали, то для їх пошуку, а також для пошуку мікрофонів підслуховуючих та записуючих пристроїв, застосовують спеціальну рентгенівську апаратуру і нелінійні локатори, випромінювання яких проникає крізь стіни, стелі, підлоги,

меблі тощо (у будь-яке місце, де можна їх заховати).

У тих випадках, коли немає приладів або немає часу на пошук радіозакладок, можна використовувати генератори перешкод для придушення закладних пристроїв.

До засобів оперативного контролю, тобто засобів виявлення факту використання радіозакладки, а іноді і її локалізації, відносять індикатори або детектори поля, частотоміри і деякі пошукові приймачі. Основна їх перевага – здатність виявляти джерела випромінювання або передавальні пристрої незалежно від типу застосовуваної в них модуляції. Принцип пошуку полягає у виявленні максимуму рівня випромінювання в приміщенні.

Класифікація та особливості експлуатації індикаторів електромагнітного поля. Найпростіший індикатор складається із ненаправленої антени лінійної поляризації, широкосмугового радіопідсилювача, амплітудного детектора і порогового пристрою, який дозволяє виявляти робочі радіозакладки, які використовують для передачі інформації практично будь-які види сигналів (рис. 9.2).

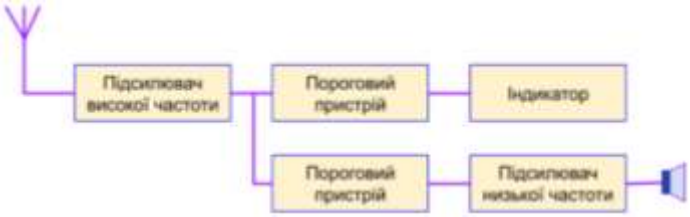

Рисунок 9.2 – Структурна схема індикатора електромагнітних випромінювань

Прилад реєструє інтегральний рівень електромагнітних випромінювань в місці прийому. У випадку, коли поточне значення перевищить встановлений поріг, який відповідає природному рівню зовнішніх випромінювань (фону), спрацьовує світлова або звукова сигналізація.

Радіозакладку можна виявити в тому випадку, якщо інтенсивність створюваного нею електромагнітного поля, перевищує рівень фону. Для підвищення здатності виявлення радіозакладок у індикаторах електромагнітного поля застосовують атенюатори, смугові та режекторні фільтри, які налаштовують на частоти потужних зовнішніх джерел та використовуються для нейтралізації впливу місцевих телевізійних і радіомовних станцій.

Введення в схему індикатора підсилювача низької частоти та гучномовця дає можливість виділити на фоні зовнішніх сигналів тестовий акустичний

сигнал, тобто реалізувати «акустичну зав'язку», суть якої полягає в наступному. Модульоване тестовим звуковим сигналом випромінювання приймається антеною індикатора, детектується та після підсилення надходить на вхід динаміка. Між мікрофоном радіозакладки і динаміком індикатора встановлюється позитивний зворотний зв'язок, який детектується у вигляді характерного звукового сигналу (у вигляді свисту).

Індикатори електромагнітних випромінювань характеризуються наступними параметрами:

– робочий діапазон частот;
– чутливість (щодо напруженості електромагнітного поля);
– радіус виявлення закладки із відомої потужністю радіопередавача;
– межі регулювання порогу чутливості, методи її підвищення;
– наявність режиму «акустичної зав'язки»;
– тип індикації;
– можливість прослуховування інформації, яку передає радіозакладка;
– тип джерела електроживлення і час безперервної роботи від нього в режимах виявлення та пошуку;
– габарити, маса, конструкція.

На практиці прийнято розрізняти наступні типи індикаторів електромагнітного поля, які класифікують за функціональними можливостями:

– малогабаритні;
– професійні;
– камуфльовані.

Єдиною функцією малогабаритних індикаторів поля є включення індикації при перевищенні рівня електромагнітного поля деякого раніше встановленого значення (порогу). Індикація таких приладів, як правило, має покажчик – «так/ні».

Деякі індикатори мають регулятор чутливості, за допомогою якого встановлюється поріг чутливості. Такі індикатори можуть застосовуватися для виявлення джерел безперервного електромагнітного випромінювання в ближній зоні (від 1 до 2 м).

Недоліками є низькі технічні показники, а також відсутність режимів ідентифікації джерела сигналу (акустозав'язки, вимірювання рівня сигналу, вимірювання частоти), невисока чутливість. Такі індикатори можуть застосовуватися для грубої локалізації джерел випромінювання.

Професійні індикатори призначені для проведення пошукових заходів, для пошуку та локалізації джерел електромагнітних випромінювань. Вони володіють

високими технічними характеристиками, широкими функціональними можливостями. Мають режим «акустичної зав'язки», регулятор чутливості, смугові фільтри, мають високу чутливість, деякі мають можливість вимірювання частоти. Дозволяють вимірювати рівень сигналу, який знаходиться в ближній зоні, мають тональну індикацію рівня сигналу «тепло/холодно». Володіють більшою кількістю переваг у порівнянні з іншими типами індикаторів поля.

Недоліком є висока ціна.

Камуфльовані індикатори призначені для прихованого застосування. Їх основною особливістю є те, що ці прилади виконані у вигляді звичайних предметів, які застосовуються в повсякденній діяльності зі збереженням їх основних можливостей.

Використання таких індикаторів не викликає підозри. Вони володіють хорошими технічними характеристиками, високою чутливістю. Деякі мають приховану індикацію («ДІ-К», «Супутник»). Перевагою є прихованість їх застосування, а недоліком – відсутність можливості ідентифікувати джерело сигналу.

В таблиці 9.1 приведено основні характеристики та функціональні можливості сучасних індикаторів електромагнітного поля.

Таблиця 9.1 – Функціональні можливості індикаторів електромагнітного поля

Модель	Діапазон частот, МГц	Акусто-зав'язка	Індикація	Примітка
1	*2*	*3*	*4*	*5*
D006	50…1000	Є	Світлодіодна шкала, звукова індикація з можливістю вимикання	
D008	50…1500	Є	Світлодіодна шкала, звукова індикація	Суміщений з приймачем для перевірки провідних комунікацій (до 500 В, 0,05-7 МГц)
PT022	30…1500	Є	Стрілочний індикатор, звукова індикація	Вбудовані смугові та режекторні фільтри
PT025	30…1500	Є	РК-дисплей, звукова індикація	Аналог PT022 + вбудований частотомір
RM-10	80…800	Нема	Світлова індикація, звукова індикація з можливістю вимикання	Можливість прихованого носіння (портмоне)

Продовження таблиці 9.1

1	2	3	4	5
ІПФ-6	30…2500	Є	РК-дисплей, звукова індикація	Смугові, режекторні фільтри, вбудований частотомір
Спутник	200…2000	Нема	Звукова індикація, віброіндикація	Закамуфльований у вигляді брелока автомобільної сигналізації
Ekostate	30…3000	Нема	Звукова індикація	Закамуфльований в авторучці
ІЕП	60…1500	Нема	Світлова та звукова індикація	Виконаний у вигляді брелока, має сторожовий режим
R-Finder	20…1500	Нема	Світлова та звукова індикація	Виконаний у вигляді брелока
ДИ-К	60…3000	Нема	Прихована світлова індикація	Закамуфльований в настільному годиннику

Детектор K18 GSM FINDER. Професійний детектор радіочастотного сигналу K18 GSM FINDER (рис. 9.3) призначений для виявлення бездротових пристроїв в діапазоні від 1 МГц до 8 ГГц.

Рисунок 9.3 – Професійний детектор радіочастотного сигналу K18 GSM FINDER

Детектор K18 GSM FINDER призначений для виявлення таких прихованих (закладних) пристроїв, як бездротові камери, мікрофони, «жучки», GPS-трекери, мобільні передавачі (2G, 3G, 4G SIM-карти).

Широкий діапазон частот дозволяє знаходити пристрої різного типу. При

цьому різні методи виявлення дозволяють виявляє камери за їх відблиском об'єктива, радіомікрофони через радіосигнал, а магнітні пристрої за допомогою давача Холла.

Вбудований дисплей та LED-індикація відображає силу випромінювання, що дозволяє точно локалізувати джерело сигналу. Звукове, візуальне та вібраційне сигналізування дозволяє сповістити про виявлення підозрілих пристроїв.

Основні технічні характеристики детектора K18 GSM FINDER:

– частотний діапазон: від 1 МГц до 8 ГГц;
– динамічний діапазон виявлення: >73 дБ;
– чутливість виявлення: 0,03 мВт;
– дальність виявлення: 1,2 ГГц – до 15 м²; 2,4 ГГц – до 10 м²; 2G, 3G, 4G – 5-15 м²;
– режим сповіщення: LED-індикація, звуковий та вібраційний сигнал;
– живлення: літій-полімерний акумулятор 3,7 В, 1200 mAh;
– час автономної роботи: 8-10 год;
– температурний режим роботи: від -10°C до +60°C;
– габаритні розміри: 138×60×28 мм;
– вага: 167 г.

Детектор Digital CC-308+. Портативний детектор Digital CC-308+ (рис. 9.4) – комбінований прилад для виявлення «жучків» та прихованих камер в діапазоні від 1 МГц до 6,5 ГГц.

Рисунок 9.4 – Портативний детектор Digital CC-308+

Детектор Digital CC-308+ прихованих камер і радіожучків, призначений для

забезпечення захисту від несанкціонованого прослуховування приміщення шляхом виявлення активності радіочастотного сигналу (GSM 850/900E/1800/1900, UMTS 850/900/1800/1900/2100, CDMA 450(A-H)/800/1900, DECT, Wi-Fi, Bluetooth) в широкому діапазоні частот від 1 МГц 6,5 ГГц, та виявлення прихованих камер, які заховано або закамуфльовано у звичайних та простих, на перший погляд предметах (картина, годинник, радіоприймач, телевізор, пожежний давач, вентиляційна решітка тощо).

Дальність виявлення детектора Digital CC-308+ до 10 метрів, а це вище за середньостатистичні детектори прихованих камер. Цього вдалося домогтися, застосувавши яскраві світлодіодні випромінювачі довжиною хвилі 920 нм.

У випадку виявлення радіочастотного сигналу, на передній панелі засвічуються червоні індикатори. Кількість засвічених індикаторів (їх є п'ять) говорить про потужність сигналу або близькості до джерела радіовипромінювання. Для того щоб звузити зону пошуку, необхідно зменшити рівень чутливості, а радіус виявлення радіочастотного сигналу залежить від потужності випромінювача.

Для візуального сканування необхідно натиснути кнопку «LED» (тоді на задній стороні включаються червоні світлодіоди) та провести огляд приміщення через віконце із червоним світлофільтром. В цьому випадку об'єктиви відеокамер будуть «засвічуватись» яскравими червоними точками.

Основні технічні характеристики детектора Digital CC-308+:

– частотний діапазон: від 1 МГц до 6,5 ГГц;
– динамічний діапазон виявлення: >85 дБ;
– чутливість виявлення радіожучків за потужності випромінювача: 50-200 мВт радіус виявлення 0,3-0,5 м; 300-600 мВт радіус виявлення 1,0-2,0 м; 800-1200 мВт радіус виявлення 3,0-10,0 м;
– радіус виявлення «жучків»: 1-15 м;
– довжина виявлення камер: 5-10 м;
– режим сповіщення: світлова індикація, звуковий сигнал;
– живлення: літієвий акумулятор 3,7 В, 45 mAh;
– температурний режим роботи: від -10°С до +50°С;
– габаритні розміри: 93×48×17 мм;
– вага: 58 г.

Детектор Protect 1206. Професійний детектор жучків Protect 1206 (рис. 9.5) – прилад, який спрямовано на протидію найсучаснішим засобам спостереження (пошук та виявлення цифрових протоколів, аналогових й цифрових малопотужних високочастотних передавачів в діапазоні від 50 МГц до 12 ГГц).

Рисунок 9.5 – Професійний детектор жучків Protect 1206

До складу детектор поля Protect 1206 входить два типи антен та два роз'єми каналів.

Перший тип антен застосовують під час роботи в частотному діапазоні від 50 МГц до 6 ГГц, що дозволяє виявляти передавальні пристрої будь-яких схем, які працюють на цих частотах (переважно усі види радіопристроїв, мікрофони, маячки, відеокамери, GSM-пристрої та інші передавальні пристрої з подібними протоколами передавання даних). Другий тип антен (Micro-Pointer) – є допоміжним пристроєм, який використовується для пошуку цифрових пристроїв із протоколами Bluetooth та Wi-Fi (передавачі, які використовують GSM, 2G, 3G, 4G, DECT і CDMA) із скануванням частот у діапазоні від 2,4 до 2,48 ГГц, від 4,9 до 5,875 ГГц.

Micro-Pointer підходить як до першого, так і до другого роз'єму. Це антена спрямованої дії з великим діапазоном частот від 2 до 12 ГГц. Основним її призначення залишається розширення можливостей приладу. Застосування цієї антени дозволяє збільшити дальність виявлення джерел з частотою понад 2 ГГц від двох до чотирьох разів, що дозволяє виявляти передавачі й відеокамери, які використовують Wi-Fi, Bluetooth, Wi-Max, LTE High та інші цифрові протоколи.

Детектор поля Protect 1206 володіє збільшеним діапазоном пошуку та змінною чутливістю (мікропроцесорне керування шкали приладу дозволяє змінювати показання поруч із потужними передавачами та слабкими сигналами). За рахунок такої властивості зменшується час пошуку шпигунського пристрою.

Прилад виконано в металевому корпусі та має світлову ідентифікацію (три кольори), яка відповідає типу передавача, звукову сигналізацію захоплення

об’єкта (чотири варіанта), шістнадцятирозрядну калібровану шкалу відображення рівня сигналу.

Основні технічні характеристики детектора поля Protect 1206:

– частотний діапазон: антена 1 (від 50 МГц до 12 ГГц); антена 2 (від 2,4 ГГц до 2,4 ГГц; від 4,9 ГГц до 5,875 ГГц);
– динамічний діапазон виявлення: від 0 до 100 дБ;
– чутливість виявлення: 2 рівня (атенюатор);
– дальність виявлення: від 10 до 15 м;
– режим сповіщення: LED-індикація, звуковий та вібраційний сигнал;
– живлення: батарея LR03 (AAA) 2×1,5 В, до 30 mAh;
– час автономної роботи: до 20 год;
– температурний режим роботи: від -10°С до +60°С;
– габаритні розміри (з антенами): 120×70×16 (210×70×16) мм.

Система пошуку закладних пристроїв Delta X G2/6. Пошукова система Delta X G2/6 (рис. 9.6) – це спеціалізований інструмент, який призначений для виявлення прихованих пристроїв (закладки, жучки та інші засоби прослуховування) в діапазоні від 9 кГц до 6(12) ГГц.

Рисунок 9.6 – Система пошуку закладних пристроїв Delta X G2/6

Пошукова система Delta X G2/6 здатна в короткі терміни швидко та надійно виявити усі види радіочастотних пристроїв негласного зняття інформації в діапазоні до 6 або 12 ГГц, включаючи аналогові, цифрові, ті які працюють постійно або періодично, передають аудіо- або відеосигнал, з шифруванням або без нього.

Delta X G2/6 дозволяє знаходити та ідентифікувати закладні пристрої, які використовують цифрові протоколи GSM, 3G, 4G/LTE, 5G, Bluetooth, Wi-Fi, DECT та інші стандарти в діапазоні до 6(12) ГГц. Дозволяє аналізувати канали Wi-Fi 2,4 ГГц, Wi-Fi 5 ГГц, Bluetooth, Bluetooth LE та Bluetooth LE Advertising.

Система пошуку закладних пристроїв Delta X G2/6 дозволяє виявляти радіочастотні подавлювачі (блокіратори, джаммери) на усіх діапазонах, включаючи діапазони мобільного зв'язку типу uplink та downlink, діапазони Глобальної Навігаційної Супутникової Системи (GPS, GLONASS, GALILEO тощо), Wi-Fi/Bluetooth.

Спектральний аналіз забезпечує високу чутливість та велику відстань виявлення (у порівнянні із радіочастотними детекторами та приймачами ближнього поля у 10-20 разів).

Функція маскування фону дозволяє відсіяти безпечні сигнали, такі як телебачення, радіомовлення, базові станції зв'язку, радіозв'язок та зосередитись на пошуку локальних сигналів які здатні створити небезпеку.

Основні технічні характеристики пошукова система Delta X G2/6:

– частотний діапазон: від 9 кГц до 6(12) ГГц;

– швидкість сканування спектру: з функцією Burst Hunt (7 ГГц/с); без Burst Hunt (11 ГГц/с);

– роздільна здатність спектру: 9.8 кГц;

– чутливість: стандартне (85 Дбм) та високе (95 Дбм) підсилення;

– динамічний діапазон: 84 Дб;

– відображуваний діапазон рівня сигналу: стандартне (від -90 до -20 Дбм) та високе (від -100 до -20 дБм) підсилення;

– полоса пропускання реального часу (RTBW): 27 МГц;

– антенні входи: INPUT (від 9 кГц до 3 ГГц); AUX1 (від 3 ГГц до 6 ГГц) та UX2 (від 6 ГГц до 12 ГГц);

– пошукові режими (час оновлення): всі сигнали (від ~0,9 с до 1,1 с); мобільні/GPS-трекери (~0,2 с); безпровідні/ISM (~0,3 с); «Низхідні/Навігація» (~0,3 с) та дослідження діапазону/сигналу (від ~0,1 с до 0,2 с);

– демодуляція: AM, FM, CW,USB, LSB зі смугою 2, 5, 15, 50, 100 та 200 кГц;

– відображувана смуга графіку спектра: від 1 МГц до 6(12) ГГц;

– час автономної роботи: від 1 до 1,5 год.;

– температурний режим роботи: від -5°C до +45°C;

– габаритні розміри без антен: 33,5×26×6 мм;

– вага з антенами (без ПК): 3,5 кг.

ХІД РОБОТИ

1. Провести, у виділеному приміщенні, пошук радіозакладного пристрою використовуючи детектор електромагнітного поля й частотомір.
2. Під час ідентифікування радіозакладки визначити її тип та у якому стані вона перебуває (увімкнена чи вимкнена).
3. За умови коли радіозакладка перебуває у робочому стані, то необхідно визначити характеристику її електромагнітного випромінювання.
4. За результатами виконаної роботи зробити висновок та підготувати звіт.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Основні типи закладних пристроїв.
2. Структурна схема закладного пристрою.
3. Демаскуючі ознаки автономних некамуфльованих акустичних закладок.
4. Демаскуючі ознаки напівактивних акустичних радіозакладок.
5. Які технічні засоби використовують для виявлення вимкнених та робочих радіозакладок?
6. Як класифікують детектори поля?
7. Методи виявлення можливих каналів витоку інформації за допомогою пошукових приладів (систем) K18 GSM FINDER, Digital CC-308+, Protect 1206 та Delta X G2/6.
8. Основне призначення та режими роботи багатофункціональних пошукових приладів K18 GSM FINDER, Digital CC-308+, Protect 1206 та Delta X G2/6.
9. Опишіть методику виявлення радіозакладних пристроїв за допомогою індикаторів електромагнітного поля.

Рекомендована література: [2; 3; 5; 11; 14; 15].

ЛАБОРАТОРНА РОБОТА №10

Тема: виявлення витоку інформації через радіозакладні пристрої, телефонні радіоретранслятори за допомогою багатофункціональних пошукових приладів та систем.

Мета: ознайомитись з методиками виявлення каналів несанкціонованого витоку інформації через радіозакладні пристрої та телефонні радіоретранслятори та підібрати пошукове обладнання для їх виявлення та локалізації.

Завдання: опрацювати теоретичний матеріал, встановити метод виявлення каналів несанкціонованого витоку інформації та підібрати пошукове обладнання.

ТЕОРЕТИЧНІ ВІДОМОСТІ

На сьогодні широкого розповсюдження набуло застосовування підслуховуючої апаратури та закладних пристроїв. Для виявлення встановлених таємно радіопередавальних пристроїв прийнято використовувати такі способи:

– пасивне виявлення (контроль радіоефіру за допомогою приймальних засобів);

– активне виявлення за допомогою радіопеленгації, яка, у свою чергу, може здійснюватися радіолокаційним зондуванням конструкцій на предмет виявлення закладних пристроїв.

Канали витоку інформації, в радіочастотному діапазоні, формуються, зазвичай, штучно (зумисно), за рахунок спеціальних технічних засобів (радіомікрофони, телефонні радіоретранслятори, несанкціоновановвімкнені радіостанції, радіомаячки тощо). У тому випадку, коли канал витоку інформації формується природно, то мова іде про побічні електромагнітні випромінювання технічних засобів опрацьовування інформації (ПК, телекси, факси тощо).

Необхідно пам'ятати і про те, що небезпечні радіосигнали можуть формуватись як внутрішніми, так і зовнішніми джерелами.

На практиці, до внутрішніх небезпечних радіосигналів відносять:

– сигнали радіозакладних пристроїв (радіомікрофони, телефонні радіотранслятори тощо);

– сигнали радіомаячків;

– сигнали несанкціоновановвімкнених у приміщенні радіостанцій та радіотелефонів;

– побічні електромагнітні випромінювання ПК та інші технічні засоби опрацювання інформації.

До категорії небезпечних необхідно відносити радіосигнали, джерелами яких можуть бути:

– радіомікрофони з виносним акустичним мікрофоном;

– телефонні радіоретранслятори, які встановлюються на лінії зв'язку за межами приміщення (але поблизу нього);

– радіостетоскопи, які встановлюють із зовнішнього боку загороджувальних поверхонь;

– винесені передавачі прихованих відеокамер;

– пристрої зовнішнього високочастотного опромінювання.

У якості джерел внутрішніх небезпечних радіосигналів доцільно розглядати електроприлади, оргтехніку, побутові засоби, а також їхні блоки живлення.

Радіомікрофони. На практиці, широкого розповсюдження набули

радіомікрофони із параметричною стабілізацією частоти передавача. Основна їх особливість – великі межі змінювання несучої частоти (до кількох МГц) тому для локалізування радіомікрофонів такого типу найбільш доцільним є застосування методу акустозав'язки.

Досить широко застосовують й радіомікрофони із кварцовою стабілізацією частоти й вузькосмуговою частотною модуляцією. Тому для пошуку й локалізації цього типу джерел найбільш доцільно використовувати амплітудний метод.

В радіомікрофонах, які призначені для встановлення в автомобільній техніці або інших транспортних засобах, виокремлюють дві основні особливості – підвищена потужність радіопередавача та більш чистий, без ознак зовнішнього фону, демодульований сигнал (за рахунок звукоізольованих властивостей корпусу автотранспорту).

Телефонні радіоретранслятори. Незважаючи на множину варіантів та різновиди виконання телефонних радіоретрансляторів можна чітко виокремити такі групи за способом їх під'єднання до елементів телефонної лінії – з гальванічним контактом та безнього. При цьому гальванічне під'єднання може здійснюватися як послідовно (у розрив одного з проводів телефонної лінії), так і паралельно (водночас до двох проводів телефонної лінії).

Телефонні радіоретранслятори послідовного ввімкнення дозволяють з'явитись в ефірі модульованого сигналу лише за умови, коли слухавка телефонного апарата піднята. У такому випадку прослуховуються сигнали АТС («виклик», «зайнято»), клацання під час набору номера, розмова абонентів після встановлення з'єднання. Локалізацію телефонних ретрансляторів даного типу доцільно здійснювати амплітудним методом. Застосовування методу акустозав'язки може призвести до помилкових висновків відносно наявності встановленого телефонного радіоретранслятора.

Телефонним радіоретрансляторам паралельного ввімкнення притаманні два різновиди.

Перший різновид передбачає реалізацію лише функції ретранслятора. При цьому в режимі піднятої слухавки на радіочастоті прослуховуються сигнали АТС («виклик», «зайнято»), клацання під час набору номера й розмова абонентів. У тому випадку коли слухавку покладено й модуляція радіосигналу відсутня, то тоді відсутньою є й сама несуча частота.

В другому різновиді часто поєднують функції телефонного радіоретранслятора й радіомікрофона. При цьому живлення забезпечується з телефонної лінії та забезпечується контроль акустики приміщення в режимі

покладеної слухавки. Такі закладні пристрої встановлюються на елементах телефонної лінії в межах контрольованого приміщення. Для їх локалізації, під час того як слухавку прокладено, використовують метод акустозав'язки із застосуванням тестового звукового сигналу. У режимі піднятої слухавки, для локалізації таких закладок, краще застосовувати амплітудний метод.

Необхідно пам'ятати, що радіоретранслятори гальванічного під'єднання, як правило, не мають власних антен, а використовують замість них провідник телефонної лінії.

Телефонні радіоретранслятори негальванічного під'єднання (індуктивного знімання інформації) можуть встановлюватись на будь-якій ділянці телефонної лінії, як правило, поза контрольованим приміщенням на абонентській лінії без порушення цілісності ізоляції провідників. Вони формують модульований радіосигнал лише під час підняття слухавки телефона. При цьому прослуховуються сигнали АТС («виклик», «зайнято»), клацання під час набору номера, розмова абонентів після встановлення з'єднання. Їх локалізація здійснюється амплітудним методом в міру обстеження телефонної лінії на усій її протяжності.

Інші джерела потенційно небезпечних радіовипромінювань. Тут необхідно розглянути, насамперед, радіостетоскопи, приховані відеокамери із радіоканалом передавання інформації, радіозакладки в ПК, радіомаячки, засоби просторового високочастотного опромінювання, несанкціоновано ввімкнені засоби зв'язку (радіостанції, радіотелефони, телефони з радіоподовжувачами).

Приховані відеокамери із радіоканалом передавання інформації відрізнюються тим, що сигнал, який випромінюється в радіодіапазоні, за структурою схожий до сигналу каналу яскравості передавачів телевізійного мовлення. Виявлення такого сигналу та локалізація його джерела здійснюється на основі амплітудного методу шляхом прослуховування змінювання тону продетектованого сигналу.

Радіозакладки в ПК призначені для передавання зображення монітора та цифрових сигналів системного блока або інших елементів фізичної архітектури комп'ютера. Основна їх особливість полягає у тому, що сигнал, який передає зображення монітора, за структурою схожий на сигнал передавача прихованої відеокамери, а в інших випадках містить усі ознаки цифрового передавання. За основу для їх виявлення та локалізації застосовують амплітудний метод, який доповнюють аналізом зображень сигналів.

Радіомаячки відрізнюються тим, що їх радіовипромінювання не володіє модуляцією акустичного фону у приміщенні (об'єкті), а є неперервним або чітко

вираженим періодичним. Можливою є модуляція тоном. Їх виявлення може здійснюватись на основі амплітудного методу у поєднанні із прослуховуванням сигналу, а локалізація відбувається лише за допомогою амплітудним методом.

Засоби просторового високочастотного опромінювання є зовнішніми й використовуються для отримання інформації із приміщень шляхом орієнтування на нього (переважно через віконні проєми) потужного чіткоспрямованого променя електромагнітного випромінювання високої частоти та приймання перевипроміненого, уже промодульованого сигналу, на частотах вищих гармонік. Основною їх особливістю під час виявлення та локалізації є те, що зондувальний сигнал є більш стабільним за частотою, а його модуляція відсутня. Зауважимо, що під час роботи спостерігається нерівномірність отримання сигналу (більш високий буде в області вікон, а низький – в коридорі та інших приміщеннях). Окрім цього, перевипромінений сигнал за частотою відповідає вищим гармонікам зондувального сигналу та має модуляцію акустичним фоном приміщення. Виявлення таких засобів здійснюється на основі амплітудного методу, який поєднують із прослуховуванням сигналу, а локалізація напрямку опромінення – лише амплітудним методом.

ХІД РОБОТИ

1. Ознайомитись із методиками виявлення каналів несанкціонованого витоку інформації через радіозакладні пристрої та телефонні радіоретранслятори.
2. Підібрати, із запропонованого пошукового обладнання, прилад для виявлення та локалізації каналу несанкціонованого витоку інформації.
3. Ознайомитись із обладнанням та алгоритмом його роботи.
4. Визначити метод виявлення можливих каналів несанкціонованого витоку інформації.
5. За результатами виконаної роботи зробити висновок та підготувати звіт.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. На основі яких способів детектують таємновстановлені радіопередавальні пристрої?
2. Як формуються канали витоку інформації в радіочастотному діапазоні?
3. Які сигнали формують групу внутрішніх небезпечних радіосигналів?
4. Джерела небезпечних радіосигналів.
5. Радіомікрофони. Типи радіомікрофонів та їх локалізація.
6. Телефонні радіоретранслятори. Види телефонних радіоретрансляторів та їх локалізація.

7. Приховані відеокамери, радіозакладки в ПК та радіомаячки, як джерела потенційно небезпечних радіовипромінювань. Виявлення та локалізація сигналу.

8. Активне та пасивне виявлення.

Рекомендована література: [2; 3; 5; 11; 14; 15].

ЛАБОРАТОРНА РОБОТА №11

Тема: застосування багатофункціональних пошукових приладів для локалізації витоку інформації через інфрачервоне випромінювання та низькочастотні магнітні поля.

Мета: ознайомитись з методиками локалізації каналів несанкціонованого витоку інформації через інфрачервоне випромінювання та низькочастотні магнітні поля, підібрати пошукове обладнання та провести їх локалізацію.

Завдання: опрацювати теоретичний матеріал та підібрати пошукове обладнання для виявлення каналів витоку інформації.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Застосування пошукових приладів/систем для виявлення каналів витоку інформації в інфрачервоному (ІЧ) діапазоні. На практиці велику увагу приділяють два види таких каналів витоку інформації. Один з них формується за рахунок застосовування спеціальних технічних засобів, за допомогою яких відбувається передача перехопленої інформації в ІЧ-діапазоні. Інший канал базується на опроміненні віконних скляних проємів спрямованим променем джерела ІЧ-випромінюваня та отримання відбитого сигналу, промодульованого акустикою приміщення. Для виявлення цих каналів витоку інформації необхідно провести однакові підготовчі заходи. Насамперед, необхідно правильно підібрати час проведення перевірки:

– необхідно дотриматись умови не потрапляння у вікно контрольованого приміщення прямих сонячних променів;

– необхідно впевнитись, що в контрольованому приміщенні вимкнені лампи розжарення та джерела інтенсивного теплового випромінювання;

– необхідно, за наявності кольорового телевізора, вимкнути його, оскільки давач пошукового приладу/системи може реагувати на теплі тони зображення.

Специфіка ІЧ-закладок визначає необхідність забезпечення прямої видимості поміж передавачем закладного пристрою та приймачем ІЧ-випромінювань. А отже, шлях слідування випромінювання передавача назовні приміщення може пролягати лише через віконні проєми. Враховуючи ці особливості пошук небезпечних сигналів необхідно розпочинати від вікон та

пересуватись в глиб приміщення. Оскільки передавач може характеризуватись досить вузькою діаграмою спрямованості, а кут огляду давача приладу становити 30°С, то тоді необхідно плавно змінювати його просторову орієнтацію.

Ознакою наявності ІЧ-випромінювання є сигналізація рівня LED-сегментів шкали індикатора пошукового приладу/системи та звуковий сигнал в режимі TONE. Необхідно зауважити, що виявлення ІЧ-сигналу може відбуватись на слух у відповідному режимі (наприклад, AUD), а також візуально, під час використання вмонтованого аналізатора спектра або осцилографа.

Локалізація джерела ІЧ-випромінювання найбільш точно відбувається під час поєднання амплітудного методу з методом акустозав'язки. При цьому порядок роботи такий же, як при роботі в режимі високочастотного детектора-частотоміра.

Для виявлення зовнішніх потенційно небезпечних ІЧ-випромінювань доцільно обстежити кожен віконний проєм. При цьому давач пошукового приладу/системи необхідно зорієнтувати в бік вікна. Плавно змінюючи його просторове положення, провести обстеження усієї площі вікона. Оскільки зондувальний сигнал не має модуляції, то його наявність може бути оцінено лише за показниками індикатора рівня та тональної індикації.

Використання приладу для виявлення каналів витоку інформації низькочастотними магнітними полями (НЧМП). Для таких каналів характерним є те, що вони формуються під час цільового застосування санкціонованих засобів (ПК, переговорні пристрої, системи звукопідсилення, магнітофони, телефони тощо). Тому за основне завдання необхідно вважати дослідження цих засобів на наявність, інтенсивність та дальність НЧМП. Варто відзначити, що поруч з цим доцільно здійснювати й пошук прихованих (несанкціоновано-прокладеної) електричних провідників/кабелів та виявляння працюючих диктофонів.

Перед проведенням робіт необхідно вимкнути в приміщенні люмінесцентні світильники, а антену приладу, за необхідністю, ввімкнути в диференційному режимі.

Потенційні джерела небезпечних НЧМП перевіряють окремо, включаючи їх у роботу по-черзі.

Під час дослідження технічних засобів доцільно оцінити дальність поширення магнітних полів та особливості їх спектра. Для цього, преш за все, магнітна антена розміщується в безпосередній близькості до досліджуваного об'єкта. За осцилограмою фіксується відносний рівень поля. Віддаляючись від

засобу дослідження та змінюючи просторову орієнтацію антени, оцінюють дальність якісного сприймання низькочастотного сигналу.

Що стосується підсилювачів звукової частоти, які мають вихідний трансформатор, то необхідно оцінити дальність якісного (розбірливого) сприймання мовного (тестового) сигналу. Таке оцінювання можна взяти за основу для правильного вибору місця для встановлення відповідних засобів на зовнішній стороні приміщення або, як варіант їх спільного розташування в приміщенні (за необхідності можна проаналізувати спектрограму).

Для пошуку прихованих електричних провідників/кабелів необхідно послідовно обійти усі стіни приміщення, розташовуючи магнітну антену в безпосередній близькості до них. Зафіксувати область зростання рівня поля й шляхом переміщення антени горизонтально та вертикально визначити проходження її прихованої траси. Щодо можливості виявлення працюючих диктофонів, то їх визначають як за рівнем магнітного поля, яке створюється їх котушками, так і за рівнем магнітного фону приміщення.

ХІД РОБОТИ

1. Ознайомитись із методиками локалізації каналів несанкціонованого витоку інформації через інфрачервоне випромінювання та низькочастотні магнітні поля.
2. Підібрати, із запропонованого пошукового обладнання, прилад/систему для виявлення та локалізації каналу несанкціонованого витоку інформації.
3. Ознайомитись із обладнанням та алгоритмом його роботи.
4. Провести локалізацію каналу несанкціонованого витоку інформації.
5. За результатами виконаної роботи зробити висновок та підготувати звіт.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Назвіть види каналів витоку інформації в інфрачервоному діапазоні та як вони формуються.
2. Які підготовчі заходи необхідно проводити перед локалізацією каналів витоку інформації в ІЧ-діапазоні?
3. Яка специфіка ІЧ-закладок?
4. Опишіть алгоритм пошуку небезпечних каналів витоку інформації які формуються низькочастотними магнітними полями та ІЧ-сигналів.
5. Чим характеризуються канали витоку інформації на базі низькочастотних магнітних полів?
6. Які підготовчі заходи проводити перед локалізацією каналів витоку інформації за низькочастотними магнітними полями?

7. За допомогою яких методів локалізують джерела ІЧ-випромінювання?

Рекомендована література: [2; 3; 5; 11; 14; 15].

ЛАБОРАТОРНА РОБОТА №12

Тема: структура та функції системи захисту інформації від несанкціонованого доступу.

Мета: ознайомитись із структурою та функціями комплексу засобів захисту інформації, яка опрацьовується на ПК, від несанкціонованого доступу.

Завдання: опрацювати теоретичний матеріал, протестувати наявну систему захисту інформації.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Комплекс засобів захисту (КЗЗ) інформації, опрацьовуваної на ПК, від несанкціонованого доступу (НСД) є спеціалізованою надбудовою над стандартною операційною системою (ОС) і доповнює її функціями розмежування доступу. Комплекс дозволяє створювати спеціалізоване робоче місце з обмеженим колом користувачів, які мають різні повноваження з доступу.

Комплекс орієнтовано на використання в організаціях для захисту конфіденційності та цілісності критичної інформації, опрацьовуваної на персональному комп'ютері в середовищі ОС MS Windows.

Програмні засоби КЗЗ є сумісні із засобами, які входять до комплекту постачання ОС, а також з іншим системним, інструментальним та прикладним програмним забезпеченням (ПЗ), яке використовує стандартні інтерфейси ОС.

Програмні засоби КЗЗ можуть бути несумісні з іншими засобами захисту від НСД, антивірусним ПЗ та з ПЗ, яке працює з дисками й файлами на низькому рівні поза файловою системою.

Структура та зміст каталогів комплексу засобів захисту. Файлова система комплексу засобів захисту складається із головного каталогу C:\--FLY--\ та інших каталогів:

- BASE\ – каталог бази даних;
- BIN\ – каталог виконуваних файлів;
- JRN\ – каталог журнальних файлів;
- HELP\ – каталог документації та файлів контекстної допомоги;
- TMP – каталог для тимчасових файлів.

У головному каталозі C:\--FLY--\ розташовується протокол інсталяції Install.log та програма деінсталяції Unwise.exe.

У підкаталозі BIN\ розташовують виконувані файли, динамічні бібліотеки,

файли ліцензій та конфігурації. До основних його файлів слід віднести наступні:

– Fly95.lic – «файл ліцензії» – містить контрольні параметри інших файлів КЗЗ;

– Flydos.sys – допоміжний системний драйвер реального режиму;

– Fly95adm.exe – VxD драйвер захищеного режиму (це ядро КЗЗ, яке виконує усі функції із розмежування доступу);

– Fly95adm.exe – автоматизоване робоче місце (АРМ) адміністратора;

– Fly95adm.ini – файл конфігурації АРМ адміністратора, який містить надбудови, які визначають конкретну політику безпеки.

Типовий зміст файлу конфігурації АРМ адміністратора має наступний вигляд:

```
[DIRS]
BaseDir=C:\--FLY--\BASE\
[COMON]
System = Grif                – назва;
Version = 1.1                – версія;
FlawControl = ON             – контроль за вихідними потоками;
Encryption = OFF             – шифрування файлів у захищених каталогах;
WipeType = Name              – затирання файлів та їхніх типів при
                               вилучанні;
InpExpControl =ON            – контроль імпортування/експортування;
ScreenSaver = ON             – блокування пристроїв введення/виведення;
SWControl = Dynamic          – контроль цілісності програмного
                               забезпечення при запусканні;
Remote Access = ON           – контроль за віддаленим доступом;
AdminRestrict = Main         – політика обмеження повноважень
                               адміністраторів:
                               Main – заборона для головного адміністратора
                               на керування БД захищених каталогів та
                               доступу до конфіденційної інформації;
                               All – заборона для всіх адміністраторів, окрім
                               головного, на редагування атрибутів інших
                               адміністраторів та надавання адміністративних
                               повноважень звичайним користувачам;
                               Add – накладання всіх заборон.
TmpAdmin = ON                – запуск АРМ адміністратора не тим
                               користувачем, який завантажив ОС;
```

TMType = ICT	– тип пристрою зчитування ідентифікаторів Touch Memory (даний файл конфігурації заборонено редагувати, оскільки ця операція призведе до порушування цілісності та блокування подальшої роботи): ICT – плата ІКТ; LPT – паралельний порт; COM2 – послідовний порт.
C4ASCX.DLL, C4PRLIBX.DLL, C4RUNX.DLL, C4TPSX.DLL	– стандартні динамічні бібліотеки СУБД Clarion (зазначені файли становлять програмну частину КЗЗ, а їх цілісність контролюється КЗЗ).

У підкаталозі BASE\ прийнято розташовувати бази даних КЗЗ. До їх складу необхідно віднести:

PQA.CSP	– файл початкових параметрів;
TCB_DB.TRS, TSB_DB	– початкова та робоча копії БД робочого місця;
USER_DB.TRS, USER.DB	– початкова та робоча копії БД користувачів;
PD_DB.TRS, PD_DB	– початкова та робоча копії БД захищених каталогів;
SW_DB.TRS, SW_DB	– початкова та робочі копії БД програмного забезпечення;
MESCOD.TRS, MESFUNC.TRS, MESSUBF.TRS	– БД кодів повідомлень для переглядання журнальних файлів;
ARMADMDB.IMM	– файл контрольних сум TRS файлів.

Всі операції із встановлення, зняття та налаштовування КЗЗ виконуються за допомогою програми Fly95adm.exe адміністраторами, які мають відповідні повноваження.

ХІД РОБОТИ

6. Ознайомитись із структурою та функціями КЗЗ від НСД, яка буде реалізована на стандартній операційній системі MS WINDOWS.

7. Визначити область застосовування КЗЗ від НСД та ознайомитись із політикою безпеки, реалізованого за допомогою цього комплексу.

8. Встановити, який функціональний профіль захисту та які вимоги рівня гарантій реалізовано КЗЗ від НСД.

9. Завантажити систему, використовуючи ім’я головного адміністратора, пароль і ключовий файл. Простежити за процедурою ідентифікування й автентифікації користувача.

10. Ознайомитись із порядком контролю цілісності КЗЗ. Запустити програму адміністрування й виконати тестування системи.

11. Ознайомитись із порядком й цілями контролю цілісності використовуваного програмного забезпечення.

12. Вивчити принципи адміністративного розмежування доступу.

13. Вивчити призначення та зміст БД захищуваних каталогів та списків доступу.

14. Створити пробний захищений каталог. Перевірити виконання режиму доступу.

15. Ознайомитись із принципом керування потоками інформації.

16. Встановити вимоги, які висуваються до середовища експлуатації, які необхідні для ефективного функціонування КЗЗ.

17. Встановити вимоги, які висуваються до фізичного середовища й персоналу. Визначити загрози інформації й типових порушників.

18. Призначити заходи запобігання завантаженню ОС без засобів захисту.

19. Скласти список необхідних налаштовувань КЗЗ.

20. Визначити шляхи обходу засобів захисту і способи їх нейтралізації.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Структура та функції комплексу засобів захисту інформації.
2. Правила та принципи ідентифікування й автентифікації користувача.
3. Роль додаткових пристроїв під час автентифікації користувача.
4. Які засоби та методи прийнято використовувати в комплексі засобів захисту з метою запобігання несанкціонованому завантаженню?
5. Призначення та склад баз даних захищених каталогів.
6. Зміст списків доступу.
7. Права доступу користувача до захищених каталогів.
8. Перерахуйте загрози інформації.

Рекомендована література: [1; 2; 4-12].

ЛАБОРАТОРНА РОБОТА №13

Тема: адміністрування та експлуатування системи захисту інформації від несанкціонованого доступу.

Мета: опанувати навички адміністрування та експлуатування комплексу

засобів захисту інформації від несанкціонованого доступу розробити криптосистему на основі шифру Цезаря.

Завдання: опрацювати теоретичний матеріал, .

ТЕОРЕТИЧНІ ВІДОМОСТІ

Адміністрування системи захисту інформації. КЗЗ інформації від несанкціонованого доступу інсталюють в ОС. Під час інсталяції було зареєстровано Головного адміністратора, а на носій інформації записано його ідентифікатор та пароль для входження адміністратора в систему.

Варто пам'ятати, що мінімальна довжина пароля − 6 символів. Допускається використання латинських літер, цифр і спеціальних символів. Будь-які три символи пароля, що слідують один за одним, не повинні повторюватися та/чи відрізнятися на одиницю.

За замовчуванням ім'я головного адміністратора – admin. Після реєстрування Головного адміністратора приймають значення налаштовувань КЗЗ, які запропоновані за замовчуванням.

У вільний слот материнської плати комп'ютера вставлено плату з мікросхемою ПЗУ, що входить до комплекту постачання.

Варто пам'ятати, що робота КЗЗ без ПЗУ допускається лише на етапі налаштовування або під час його відновлення після аварії (наприклад за виходу ПЗУ з ладу) і розглядається як позаштатна ситуація. Оскільки за відсутності ПЗУ існує ймовірність завантаження ОС без засобів захисту, то опрацювання критичної інформації за відсутності ПЗУ є неприпустимим.

Порядок завантаження системи. Під час завантаження системи адміністратор має переконатись, що в цей час не виникає жодних конфліктів, і що програми ПЗУ включено до роботи.

У відповідь на запити КЗЗ слід увести свої ім'я й пароль. У ході введення ім'я й пароля доцільно дотримуватись регістра введення усіх символів. У разі помилки використовують клавіші «Esc» або «Backspace», що дозволяє повторного видати запит. Введення імені та пароля завершується натисканням клавіші «Enter». Наприклад:

Username > admin

Password > ******

Після повідомлення «Insert ID device and press <Enter> when ready» необхідно вставити завантажити з носія інформації ідентифікатор та натиснути клавішу «Enter».

Аби переконатися, що програми ПЗУ включено до роботи, слід простежити за появою запиту імені й пароля користувача до видання повідомлення «Starting

Windows».

Реєстрування додаткових користувачів. Для реєстрації додаткових користувачів прийнято виконувати наступні дії:

– завантажується АРМ адміністратора;

– викликається діалог роботи з БД користувачів за допомогою «іконки» на панелі інструментів або пункт меню «Користувачі/Облікові записи»;

– вводиться ім'я користувача та задаються інші необхідні атрибути;

– зберігається введений запис;

– вставляється новий ідентифікатор у пристрій зчитування, вводиться та затверджується пароль користувача.

Під час виконання цієї операції варто пам'ятати про таке:

– не можна використовувати один і той самий ідентифікатор для різних користувачів;

– для роботи із захищеними каталогами потрібен хоча б один адміністратор, окрім головного, котрий мав би повноваження роботи з БД захищених каталогів і допуск «ТАЄМНО»;

– на етапі налаштовування КЗЗ для користувачів рекомендується встановлювати «м'який режим» реагування на НСД, що згодом під час переходу до штатної роботи слід заборонити;

– не слід встановлювати надто докладне реєстрування подій, оскільки тоді журнальні файли КЗЗ займатимуть дуже багато місця на диску;

– допуск інших користувачів слід задавати відповідно до рівня конфіденційності інформації, до якої вони потенційно можуть мати доступ.

Створення пробного захищеного каталогу. Для створення пробного захищеного каталогу необхідно виконати такі операції:

– завантажити АРМ адміністратора з повноваженнями користувача, який має повноваження роботи з БД захищених каталогів;

– викликати діалог роботи з БД захищених каталогів, використовуючи «іконку» на панелі інструментів або пункт меню «Каталоги». Обрати в дереві каталогів гілку «ДСП» або «ТАЄМНО» і натиснути кнопку «Створити»;

– обрати ім'я каталога й натиснути кнопку «Зберегти». У якості захищеного каталогу не можна обирати кореневий каталог диска;

– натиснути кнопку «Користувачі» й задати користувачів, котрі мають права доступу до даного каталогу та вказати вид доступу (лише читання або читання/запис).

Встановлення необхідних налаштовувань КЗЗ. Для встановлення налаштовувань КЗЗ прийнято виконувати наступні дії:

– завантажується АРМ адміністратора з повноваженнями головного адміністратора;

– викликається діалог «Налаштовування системи» за допомогою пункту меню «Система/Налаштовування». Обирається закладка «Ресурси»;

– для заблоковування можливості копіювання конфіденційної інформації у відкриті каталоги встановлюється прапорець «Контроль вихідних потоків»;

– для заблоковування можливості несанкціонованого здобуття конфіденційної інформації шляхом «збирання сміття» встановлюється прапорець «Затирати вміст файлів при вилучанні» та «Затирати імена файлів при вилучанні». Використання даної функції сповільнює процес вилучання файлів у захищених каталогах і унеможливлює їхнє відновлювання за випадкового вилучання.

Встановлення режиму контролю цілісності програмного забезпечення. Для встановлення режиму контролю цілісності програмного забезпечення (ПЗ) прийнято виконувати наступні дії:

– вилучається з дисків зайве ПЗ;

– завантажується АРМ адміністратора з повноваженнями головного адміністратора;

– викликається діалог роботи з БД захищених каталогів за допомогою «іконки» на панелі інструментів чи пункт меню «Програми» й натискається кнопка «Реєстрація»;

– у діалозі «Майстер реєстрації» у лівому верхньому списку каталогів обирається кореневий каталог диска С натискаючи відповідну кнопку, яка розташована праворуч від дерева каталогів. У правому вікні з’явиться список програмних модулів, знайдених на диску. Встановлюється праворуч угорі перелік контрольованих параметрів і натискається кнопка «Зареєструвати»;

– операція повторюється для всіх логічних дисків;

– викликається діалог «Налаштовування системи» за допомогою пункту меню «Система/Налаштовування», обирається закладка «Ресурси» і встановлюється прапорець «Контролювати цілісність ПЗ при запусканні».

Моделювання планованої технології роботи. З метою моделювання планованої технології роботи на практиці прийнято контролювати роботу КЗЗ за журналами. Для цього:

– завантажують АРМ адміністратора із повноваженнями головного адміністратора;

– викликають діалог роботи з БД захищених каталогів за допомогою «іконки» на панелі інструментів або пункту меню «Журнали»;

– обирають у списку журнал за потрібну дату й натисніть кнопку «Перегляд»;

– переглядають журнал (повідомлення про НСД позначаються червоними «іконками» зі знаком оклику чи зірочкою, а синім за умов «м'якого режиму»).

У разі виникнення конфліктів та/чи повідомлень про спроби НСД установіть коректні налаштовування КЗЗ, права доступу користувачів, їх повноваження тощо.

У тому випадку коли буде проведено випробування технології роботи й визначено необхідні налаштовування КЗЗ і права доступу користувачів, то тоді можна розпочинати роботу із реальною інформацією (при цьому, не варто забувати про вимикання для користувачів «м'якого режиму» реагування на НСД).

Експлуатування системи захисту інформації. В основному, робота користувача на ПЕОМ у захищеному середовищі здійснюється так само, як на звичайному ПК. Проблемами захисту на спеціалізованому робочому місці займається адміністратор. При цьому користувачеві слід чітко слідувати його вказівкам. Адміністратор має проінструктувати користувача про встановлені правила роботи, права користувача, обов'язки й обмеження.

У свою чергу, про всі помічені відхилення від штатної роботи (відсутність чи поява незрозумілих повідомлень, особливо в процесі завантажування, змінення поводження системи при доступі до захищених каталогів тощо) користувач зобов'язаний негайно повідомляти адміністраторові.

Входження до системи. Процес входження до системи має розпочинатись із ввімкнення живлення чи перезавантаження ОС (гарячого чи холодного). Якщо користувач, підійшовши до ПЕОМ, бачить, що ще не завершено попередній сеанс роботи, його слід завершити неодмінно. Якщо користувач, підійшовши до ПЕОМ, бачить на екрані запит імені й пароля, йому не слід покладатися на те, що це запити засобів захисту, а обов'язково перезавантажити ПЕОМ.

Завантаження ОС легітимним користувачем. При завантаженні ОС засоби захисту здійснюють ідентифікування й автентифікацію користувача. Для цього користувача просять ввести ім'я (username) і пароль (password), а також надати/пред'явити переносний ідентифікатор (Touch Memory) або «ключовий диск». Переносний ідентифікатор, а також пароль для першого входження до системи користувачеві надає адміністратор.

Завантаження ОС відбувається в такий спосіб. При ввімкненні живлення, холодному чи гарячому перезавантаженню перед завантаженням ОС надсилається запит «Username >», у відповідь на який слід ввести ім'я

користувача. Під час введення імені та паролю необхідно дотримуватись регістра при введенні всіх символів. У разі помилки користувач має натиснути клавішу «Esc» чи «Backspace», що призведе до повторного видання запиту. Введення імені завершується натисканням клавіші «Enter». Після цього надсилається наступний запит – «Password >», у відповідь на який користувач повинен увести свій пароль. Початковий пароль надається адміністратором при реєструванні користувача й має бути змінений користувачем при першому ж входженні до системи. При введенні пароля на екрані замість символів, що вводяться, відбиваються «зірочки». Введення пароля також завершується натисканням клавіші «Enter». Після введення пароля надсилається повідомлення «Insert ID device and press <Enter> when ready», у відповідь на яке слід вввести ідентифікатор до зчитувача. Якщо у якості переносного ідентифікатора користувач використовує «ключовий диск», то він вставляє його у USB роз'єм, а якщо ідентифікатор Touch Memory – то у зчитувач, після чого натискає клавішу «Enter». Після цього здійснюється пошук ідентифікаторів (у такому порядку: Touch Memory, диск) й читання першого відзнайденого ідентифікатора.

Приклад діалогу при входженні до системи:

Username > admin
Password > ******
Insert ID device and press <Enter> when ready
..... Search for TM .....

У разі введення коректної інформації на короткий час надсилається повідомлення «Access granted» (доступ дозволено) – і процес завантаження системи триває.

Під час подальшого завантаження відбувається наступне:

– надсилається повідомлення ОС «Starting Windows»;

– здійснюється опрацювання файла CONFIG.SYS, при цьому надсилаються діагностичні повідомлення «IKT-ROM Present» (ПЗУ КЗЗ є присутнім), вітання «<username>, you welcome» (Користувач такий-то, завжди Вам раді) і «Device FLYDOS loaded2 (Драйвер КЗЗ завантажено);

– здійснюється опрацювання файла AUTOEXEC.BAT (якщо він є).

Якщо апаратний захист від несанкціонованого завантаження (НЗЗ) не встановлено, то ідентифікування й автентифікація користувача здійснюються драйвером FLYDOS.SYS – після повідомлення «IKT-ROM absent» (ПЗУ відсутній) видаються запити імені й пароля. Однак, подальше завантаження відбувається лише в тому разі, якщо користувач має привілей «Завантаження без ПЗУ», а до жорсткого диску (ЖД) буде внесено відповідний запис про НСД. Про

дану ситуацію слід довести до відома адміністратора КЗЗ.

Робота КЗЗ без ПЗУ розглядається як позаштатна ситуація. Опрацювання критичної інформації за відсутності ПЗУ є неприпустиме. У разі видання системою повідомлень про відсутність ПЗУ – користувач повинен негайно довести це до відома адміністратора.

Спроби несанкціонованого завантаження. У разі повторення більш двох разів некоректного введення імені чи пароля користувача, або пред'явлення підробленого ідентифікатора видається повідомлення «Access denied. System halted» (Доступ заборонено. Зупин системи) – і здійснюється зупин системи (завантаження припиняється).

Перевіряння терміну чинності повноважень. Коли адміністратор реєструє користувача в системі, він задає термін закінчення чинності його повноважень і пароля. Коли користувач змінює свій пароль, термін закінчення чинності пароля встановлюється автоматично (за замовчуванням – три місяці).

Під час завантаження КЗЗ порівнює поточну дату з датами закінчення терміну чинності пароля і повноважень, і за сім днів до закінчення терміну чинності попереджає про це, видаючи відповідно повідомлення «Your account is about to expirate. Call admin» (Термін чинності Вашого облікового запису минає. Зверніться до адміністратора) чи «Your password is about to expirate. Change it» (Термін чинності Вашого пароля минає. Замініть його). У першому випадку користувачеві слід звернутися до адміністратора, а в другому – замінити пароль.

Якщо термін чинності повноважень чи пароля минув, то буде видане повідомлення «Your account is expirate. Access denied. System halted» (Термін чинності Вашого облікового запису минув. Доступ заборонено. Зупин системи) чи «Your password is expirate. Access denied. System halted» (Термін чинності Вашого пароля минув. Доступ заборонено. Зупин системи), відповідно, – і користувач не зможе ввійти до системи. У цьому разі користувачеві слід звернутися до адміністратора.

Окрім того, КЗЗ допускає входження користувача в систему лише в ті дні тижня й години дня, в які йому це дозволено адміністратором. Якщо користувач спробує ввійти до системи в той день тижня чи в той час, коли це йому не дозволено, то КЗЗ видасть повідомлення «Your come at a wrong date/time. Access denied. System halted» (Ви прийшли не в той день/невчасно. Доступ заборонено. Зупин системи). У цьому разі користувачеві також слід звернутися до адміністратора.

Перевіряння цілісності КЗЗ. У перебігу завантаження КЗЗ виконує перевіряння цілісності свого ПЗ. У разі виявлення порушування цілісності

подальше завантаження ОС припиняється зі стандартним повідомленням про те, що живлення комп'ютера можна вимкнути. У даній ситуації необхідне втручання адміністратора.

Змінення пароля. Користувач має змінити пароль при першому ж входженні до системи, інакше, зареєструвавши, його адміністратор зможе входити до системи і працювати під його ім'ям.

Пароль має обмежений термін чинності, тому періодично його слід змінювати. Про необхідність змінення пароля свідчить видаване при завантаженні ОС повідомлення «Your passwordis about to expirate. Change it» (Термін чинності Вашого пароля минає. Замініть його).

Для змінення пароля слід запустити з каталогу C:\-iFLY-BIN\ програму FLY95ADM.EXE і обрати підпункт «Пароль» пункту «Користувачі» основного меню. Після цього програма попросить користувача пред'явити ідентифікатор, що носиться, (під'єднати диск чи піднести ідентифікатор ТМ до зчитувача), і запросить старий (чинний) пароль для входження до системи. У відповідь на це слід ввести чинний пароль у діалозі введення пароля. При введенні правильної інформації стає активним діалог уведення нового пароля. Слід ввести, а потім потвердити новий пароль, після чого програма знову попросить піднести переносний ідентифікатор, до якого вона занесе необхідну інформацію.

Мінімальна довжина пароля для входження до системи є 6 символів, максимальна – 16. Окрім того, забороняється використовувати тривіальні паролі. Правила перевіряння пароля на тривіальність включає у себе:

– будь-які три підряд символи пароля не повинні повторюватися;

– будь-які три підряд символи пароля не повинні відрізнятися від попередніх на одиницю.

Під час обирання пароля можна керуватися наступними правилами:

– обирати свій пароль таким, аби його було легко запам'ятати, а іншим складно добрати;

– не використовувати за пароль своє ім'я чи прізвище, імена й прізвища (у тому числі дівочі) рідних, клички домашніх улюбленців, дні народження й інші знаменні дати;

– уникати використання географічних назв і, взагалі слів, що вони зустрічаються в словниках, у тому числі слів, доповнених певною літерою, іноземних слів, набраних українською мовою, й навпаки, тощо;

– оптимальний вибір – пароль, що він являє собою перші літери слів, котрі складають приказку чи крилатий вираз, «розведений» спеціальними символами (розділовими знаками, символами арифметичних операцій тощо) та/чи цифрами

(лише не слід забувати, який саме вираз було обрано і де «повтикано» розділові знаки).

Окрім того, слід пам'ятати, що інформація автентифікування (пароль і вміст ідентифікатора, що носиться,) на відміну від інформації ідентифікування (імені) є «таємною» інформацією і не повинна бути відома та/чи доступна нікому, окрім користувача, якому вона належить. Тому, необхідно дотримуватись наступних правил:

– не залишайте свій переносний ідентифікатор без догляду й ніколи й нікому його не передавайте;

– ніколи й нікому не повідомляйте свого пароля;

– ніколи й ніде не записуйте свого пароля.

Якщо усе зроблено правильно, то новий пароль набирає чинності. Його слід буде вводити у відповідь на запит «Password >» при завантажуванні системи.

Робота із захищеними каталогами. Адміністратор має проінформувати користувача про те, які каталоги є захищеними і які права доступу до них користувач має. Адміністратор визначає так само можливість використання змінних носіїв (дисків).

Користувач не повинен копіювати файли із захищених каталогів, до яких він має доступ, у незахищені. Вони не для того захищаються, аби потім будь-хто мав змогу їх читати. Такі дії відстежуються й блокуються КЗЗ та контролюються по журналах.

Користувач не повинен виконувати жодних операцій з файлами в каталогах КЗЗ.

Наявність права щодо читання захищеного каталогу дає користувачеві можливість переглядати вміст каталогу і його підкаталогів, читати файли, переглядати атрибути файлів і запускати на виконання програми, які розміщено в даному каталозі та його підкаталогах.

Наявність права щодо записування до захищеного каталогу надає користувачеві можливість редагувати й вилучати в даному каталозі та його підкаталогах файли й їхні атрибути, а також перейменовувати ці файли й підкаталоги.

Окрім того, при роботі із захищеними каталогами діє таке обмеження: КЗЗ забороняє здійснювати перейменування і вилучання захищеного каталогу й тих каталогів, що його містять, аж до диска, що він перебуває в корневому каталозі.

Усі спроби несанкціонованого доступу до захищених каталогів фіксуються в спеціальних журналах і про них повідомляється адміністраторові.

Робота із змінними носіями та виведення інформації на друк.

Адміністратор має право обмежити доступ до змінних носіїв інформації, через які може здійснюватися імпортування/експортування інформації, а також виведення на друк. У цьому разі він має поінформувати користувача про те, які каталоги є каталогами імпортування/експортування й чи має користувач до них доступ, а також чи може користувач роздруковувати інформацію. Користувач має погоджувати з адміністратором порядок використання змінних носіїв (дисків).

Запускання програм. У КЗЗ реалізовано функцію контролю цілісності прикладного програмного забезпечення. Якщо її задіяно, то користувач не може запускати на робочому місці сторонні програми, у тому числі й зі змінних носіїв.

Усі подібні дії розглядаються як несанкціоновані, фіксуються в спеціальних журналах і про них повідомляється адміністраторові.

Блокування клавіатури. У КЗЗ реалізовано можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші й монітора). Блокування здійснюється чи користувачем за допомогою певної комбінації клавіш (Ctrl-Alt-F11> чи <CtrlAlt-F12>), чи КЗЗ за бездіяльності користувача в плині визначеного адміністратором періоду часу.

У стані блокування маніпулятор «миша» вимикається, екран гаситься й на нього виводиться попереджувальне повідомлення й запит пароля («Password >»). Будь-яке натискання клавіші на клавіатурі сприймається як уведення символу пароля. Робота фонових програм при цьому може тривати.

Для розблокування комп'ютера користувачеві треба пред'явити свій переносний ідентифікатор, і ввести свій пароль. Розблоковувати пристрій інтерфейсу користувача може лише той користувач, що він завантажив ОС у даному сеансі.

Забороняється вимикати живлення ПЕОМ у стані блокування, – це може призвести до втрати інформації.

Завершення роботи. Після того, як користувач завершив роботу на ПЕОМ і планує вийти, йому слід неодмінно завершити свій сеанс роботи, у противному разі будь-яка людина, що підійшла, зможе здійснювати доступ до інформації з правами користувача, який не завершив свого сеансу роботи. Завершення сеансу роботи здійснюється штатними засобами Windows, наприклад за допомогою вибору кнопки «Пуск» і пункту «Завершення роботи.../Вимкнути комп'ютер». Про нормальне завершення сеансу роботи свідчить поява напису «Тепер живлення комп'ютера можна вимкнути».

Перезавантаження в режимі емуляції MS-DOS (з використанням пункту «Перезавантаження в режимі MS-DOS» меню «Завершення роботи Windows»)

для користувачів заборонено. Спроба виходу до режиму емуляції MS-DOS завершується примусовим перезавантаженням ОС.

ХІД РОБОТИ

1. Адміністрування системи захисту інформації:

1.1 Повторити структуру й функції КЗЗ від НСД, яка реалізована у стандартній ОС.

1.2 Визначити й спланувати технологію роботи на спеціалізованому робочому місці із обмеженим колом користувачів, яких наділено різними повноваженнями із доступу до ресурсів.

1.3 Встановити, які засоби та методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню.

1.4 Завантажити систему, використовуючи ім'я головного адміністратора, пароль і ключовий ідентифікатор.

1.5 Зареєструвати додаткових користувачів.

1.6 Створити пробний захищений каталог. Перевірити виконання режиму доступу до нього.

1.7 Скласти список необхідних налаштовувань КЗЗ. Установити необхідні налаштовування КЗЗ.

1.8 Встановити режим контролю цілісності ПЗ.

1.9 Змоделювати плановану технологію роботи.

2. Експлуатування системи захисту інформації:

2.1 Повторити структуру КЗЗ, який реалізовано в стандартній операційній системі MS WINDOWS.

2.2 Визначити і сформулювати правила розмежування доступу при роботі на спеціалізованому робочому місці з обмеженим колом користувачів, наділених різними повноваженнями з доступу до ресурсів.

2.3 З'ясувати, які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню.

2.4 Здійснити входження до системи використовуючи надані адміністратором ім'я, пароль та «ключовий диск»:

– випробувати дію системи перевіряння терміну чинності повноважень користувача;

– змінити пароль користувача;

– дослідити можливості роботи користувача в захищених каталогах (способи документування роботи користувача в системних журналах);

– розглянути правила роботи зі змінними носіями і виведенням на друк;

– перевірити, чи може користувач запускати сторонні програми;

– виконати блокування й розблокування інтерфейсних пристроїв комп'ютера;

– виконати коректне завершення роботи.

ЗАПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

1. Структура та функції комплексу засобів захисту інформації стандартної операційної системи.
2. Як переконатись у правильності завантаження комплексу засобів захисту інформації?
3. Реєстрування додаткових користувачів та вимоги, які висуваються до цієї процедури.
4. Які існують обмеження при роботі із захищеними каталогами?
5. Як установити необхідні налаштовування комплексу засобів захисту інформації?
6. Які налаштовування комплексу засобів захисту інформації є необхідними (у відповідності до політики безпеки)?
7. Яким чином можна запобігти можливості копіювання конфіденційної інформації у відкритих каталогах та можливості несанкціонованого здобуття конфіденційної інформації?
8. Правила розмежування доступу під час роботи на спеціалізованому робочому місці із обмеженим колом користувачів, яким надано різні повноваженнями з доступу до ресурсів.
9. Що відбувається під час спроби несанкціонованого завантаження?
10. Які обмеження накладаються на термін чинності повноважень користувача?
11. Поясніть принципи перевіряння цілісності програмного забезпечення комплексу засобів захисту інформації.
12. Права доступу користувача до захищуваних каталогів.

Рекомендована література: [1; 2; 4-12].

ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Вакалюк Т. А. Захист інформації в комп'ютерних системах. URL: http://eprints.zu.edu.ua/9650/1/1.pdf (дата звернення: 09.04.2025).
2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Голев Д. В., Русляченко О. Ю., Бєлова Ю.В., Гончарук Д. С. Інформаційна безпека інформаційно-комунікаційних систем: навча. посіб. Лабораторний практикум. Частина 2. Комплекси технічного захисту інформації. URL: https://surl.li/wzxgbb (дата звернення: 09.04.2025).
4. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. URL: https://surl.li/jhtjql (дата звернення: 09.04.2025).
5. Гуз А. М. Організація захисту інформації з обмеженим доступом. URL: http://za.inf.ua/bo/oziod18.pdf (дата звернення: 09.04.2025).
6. Заплотинський Б. А. Основи інформаційної безпеки. URL: http://surl.li/pfkpnk (дата звернення: 09.04.2025).
7. Захарченко М. В., Кононович В. Г., Кільдішев В. Й., Голев Д. В. Інформаційна безпека інформаційно-комунікаційних систем: навч. посіб. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД. URL: https://surl.lu/pwwfqa (дата звернення: 09.04.2025).
8. Інформаційна безпека / за ред. Ю. Я. Бобала та І. В. Горбатого. URL: http://surl.li/iglfxk (дата звернення: 09.04.2025).
9. Інформаційна безпека : підруч. / за ред. В. Остроухова. К. : Вид-во Ліра-К, 2021. 412 с.
10. Кавун С. В. Носов В. В. Манжай О. В. Інформаційна безпека : навч. посіб. URL: http://surl.li/ikprgx (дата звернення: 09.04.2025).
11. Комплексні системи захисту інформації. URL: http://surl.li/yptezr (дата звернення: 09.04.2025).
12. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf (дата звернення: 09.04.2025).
13. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління. URL: http://surl.li/znnide (дата звернення: 09.04.2025).
14. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації : навч. посіб. / за ред. Іванченко С.О. URL: https://surl.li/gbotjj (дата звернення: 09.04.2025).
15. Чобаль О. І., Трикур І. І., Самохвалов М. П., Різак В. М. Методи і засоби захисту інформації: лабораторний практикум. Ужгород: ДВНЗ Ужгородський національний університет. 2023. 80 с.

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Апаратні та програмні засоби захисту інформації: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 68 с.

Комп'ютерний набір та верстка: Олег КАЙДИК.

Редактор: в авторській редакції.

Підп. до друку «__» _____ 2025 р.
Формат 60x84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 4,3. Обл. – вид. арк. 3,9.
Тираж _50_ прим. Зам. _____.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75