Міністерство освіти і науки України
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій

МЕТОДИЧНІ ВКАЗІВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ З ДИСЦИПЛІНИ "ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ"

для студентів денної та заочної форм навчання
спеціалності "Комп'ютерна інженерія"

Тернопіль 2022

Методичні вказівки до виконання лабораторних робіт з дисципліни “Захист інформації в комп’терних системах і мережах” / Н.Я. Савка, Л.О. Дубчак / Під ред. О.М. Березького. Тернопіль: ЗУНУ, 2022. 31 с.

Укладачі: Н.Я. Савка, к.т.н., доцент кафедри комп’ютерної інженерії, Західноукраїнський національний університет
Л.О. Дубчак, к.т.н., доцент кафедри комп’ютерної інженерії, Західноукраїнський національний університет

Відповідальний за випуск: Березький О.М., д.т.н., професор, завідувач кафедри комп’ютерної інженерії, Західноукраїнський національний університет

Рецензенти: Луцик І.Б., к.т.н., доцент кафедри комп’ютерних технологій, Тернопільський національний педагогічний університет

Мельник А.М., к.т.н., доцент кафедри комп’ютерних наук, Західноукраїнський національний університет

Методичні вказівки розглянуто та рекомендовано до друку на засіданні кафедри комп’ютерної інженерії протокол № 8 від 25 березня 2022 р.

Методичні вказівки затверджено на засіданні групи забезпечення спеціальності "Комп’ютерна інженерія" протокол № 5 від 25 берзня 2022 р.

ЗМІСТ

ВСТУП

Інформаційні ресурси в сучасних умовах є одним із найважливіших результатів діяльності людського суспільства. Саме тому особливу увагу приділяють задачі захисту інформації. Особливої актуальності така задача набуває в умовах стрімкого розвитку інформаційних технологій. Такі технології з кожним роком залучають все більшу частину інформаційних ресурсів в процес електронної обробки, що в свою чергу призводить до підвищення вимог щодо параметрів програмно-апаратних засобів, які використовують для захисту.

З іншого боку, відбувається розвиток нових систем захисту, побудованих на традиційних підходах. При цьому збільшується кількість та різнорідність кінцевих користувачів, яких залучають до обробки інформаційних ресурсів. Також варто зазначити, що у процесі обробки інформації використовують розподілені, неоднорідні комп'ютерні системи та мережі, політика безпеки яких суттєво відрізняється одна від одної. Зазначені аспекти створюють нові передумови щодо розробки методів та засобів захисту інформаційних ресурсів від постійно змінних різноманітних загроз.

Розроблені методичні вказівки призначені для студентів спеціальності «Комп'ютерна інженерія», які займаються проблемою захисту інформації в комп'ютерних системах і мережах із застосуванням програмних засобів.

ЛАБОРАТОРНА РОБОТА №1
ШИФРУВАННЯ ФАЙЛІВ ТА ПАПОК ЗАСОБАМИ SECURE IT.

Мета: ознайомитися з програмним засобом, який здійснює шифрування та дешифрування файлів і папок симетричними криптоалгоритмами.

Хід роботи

1. Ознайомитись із документацією Secure IT.
2. Здійснити опис симетричних криптоалгоритмів, на основі яких здійснюють шифрування та дешифрування даних.
3. Вибрати файл для реалізації шифрування.
4. Слідуючи підказкам Secure IT, здійснити шифрування файлу двома різними алгоритмами з використанням одного і того ж ключа. Вихідний файл після здійснення першого шифрування залишити, а після другого видалити повністю (без збереження в «корзині»).
5. Порівняти розмір шифрованих файлів.
6. Здійснити дешифрування хоча б одного з отриманих файлів.
7. Зашифрувати файл у *.exe файл засобами Secure IT із застосуванням стиснення до мінімальних розмірів. Порівняти його розмір з попередніми зашифрованими файлами.
8. Підготувати звіт.

Контрольні запитання

1. Якими криптоалгоритмами здійснюють шифрування та дешифрування у Secure IT?
2. Які основні відмінності застосованих криптоалгоритмів?
3. Ключ якої довжини необхідно застосовувати у Secure IT? Чому?
4. Як здійснюється шифрування засобами Secure IT?
5. Як здійснюється дешифрування засобами Secure IT?

6. Як здійснити повне знищення вихідного файлу після шифрування?

7. Яка відмінність між зашифрованим файлом та зашифрованим *.exe файлом?

Структура звіту

1. Описати процес шифрування та дешифрування вибраного файлу різними способами, зазначеними вище.
2. Порівняти розмір отриманих файлів.
3. Здійснити опис процесу дешифрування файлу.
4. Зробити висновки.

ЛАБОРАТОРНА РОБОТА №2
ЗАХИСТ ТЕКСТОВИХ ДОКУМЕНТІВ В MICROSOFT WORD

Мета: отримати навики захисту текстової інформації.

Теоретичні відомості

У Microsoft Word існує можливість захисту створеного документа від доступу до нього інших користувачів. Для захисту слід встановити пароль, який програма Word запитуватиме кожного разу під час відкриття документа. Можна також встановити захист від змін у документі. Обидва ступені захисту забезпечуються окремими паролями.

Спочатку слід відкрити вікно документа, для якого встановлюється захист і виконати усі можливі випадки захисту документа. Для цього виконують таку послідовність кроків. У відкритому документі Microsoft Word переходять на вкладку Файл. Відкривається вікно, що зображено на рисунку 2.1.

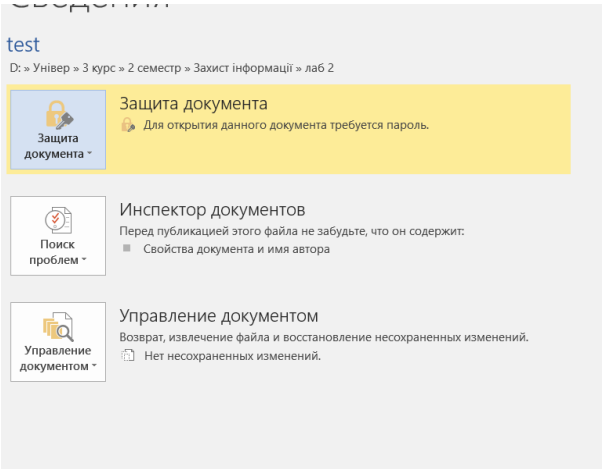

Рисунок 2.1 – Екранна форма вікна для захсту документа

Після цього вибираємо тим захисту (див. рис. 2.2). Варто дослідити усі типи захисту.

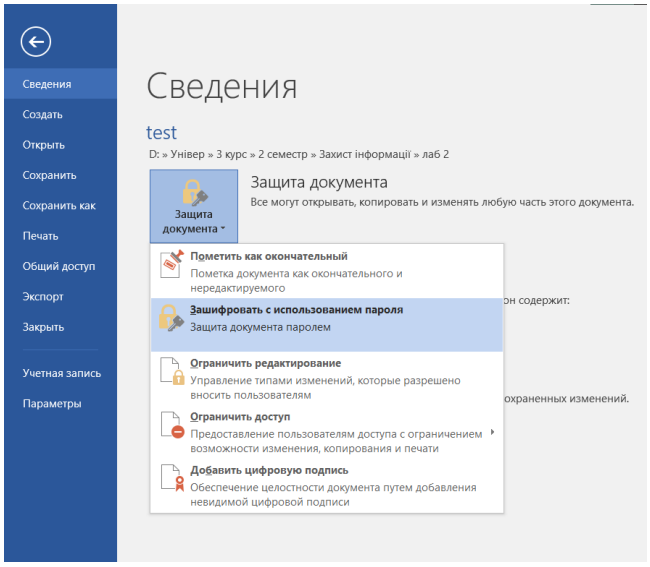

Рисунок 2.2 – Екранна форма вікна вибору типу захисту документа

Для пароля застосовують довільні сполучення літер, цифр і пробілів завдовжки не більш 15 символів. Під час запису пароля істотним є регістр (великі або малі літери).

Далі необхідно клікнути по кнопці **ОК** і в наступному діалозі підтвердити пароль його повторним набором. Якщо задаються два паролі, то один за одним з’являються два діалоги, в яких потрібно набрати пароль і натиснути кнопку **ОК**.

Тепер кожного разу під час відкриття документа програма запитуватиме у пароль. Без введення пароля документ неможливо буде завантажити.

Для зміни або видалення пароля потрібно повторити описану вище процедуру. В поле пароля вводиться нове значення або видаляється клавішею **Delete**.

Хід роботи

1. Створіть текстовий документ у редакторі Microsoft Word.
2. Захистіть створений документ від змін одним паролем.
3. Захистіть документ від відкривання, застосовуючи інший пароль.
4. Оформіть звіт про виконання лабораторної роботи.

Контрольні запитання

1. Які можливості захисту текстового документу у редакторі Microsoft Word?
2. За допомогою якої вкладки здійснюється захист документу?
3. З яких символів може складатися пароль?
4. Яка максимальна кількість символів може бути в паролі?
5. Яка мінімальна кількість символів пароля забезпечує захист інформації?

ЛАБОРАТОРНА РОБОТА №3
ЗАХИСТ ІНФОРМАЦІЇ ЗАСОБАМИ ОС WINDOWS

Мета: Дослідити стандартні засоби захисту інформації та отримати навики адміністрування ОС Windows.

Теоретичні відомості

На даний час поширеними операційними системами (ОС), які використовуються користувачами персональних комп'ютерів, є Windows 8, Windows 10. Ці ОС мають багато засобів захисту інформації та адміністрування, що забезпечує збереження даних від несанкціонованого доступу.

Найголовнішим засобом захисту даних ОС є адміністрування, тобто надання привілеїв користувачам системи. На рисунку 3.1 предствлено екранну форму вікна із переліко усіх можливих засобів адміністрування в системі Windows 10.

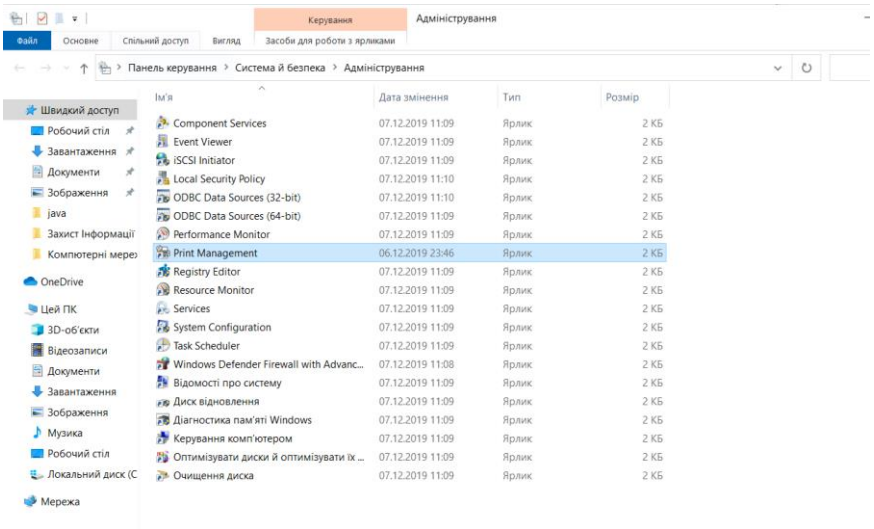

Рисунок 3.1 – Перелік усіх можливих засобів адміністрування

Крім цього існує опція «Батьківський контроль», що дозволяє обмежити не тільки доступ до певних даних, а й час користування ПК. На рисунку 3.2 показано екранну форму вікна для створення облікового запису дитини із налаштуваннями батьківського контролю.

Управління обмеженнями для облікового запису дитини здійснюється онлайн при вході з облікового запису батька на account.microsoft.com/family (потрапити на цю сторінку можна також з ОС Windows через Параметри – Облікові записи – Сім'я і інші користувачі – Управління сімейними налаштуваннями через Інтернет).

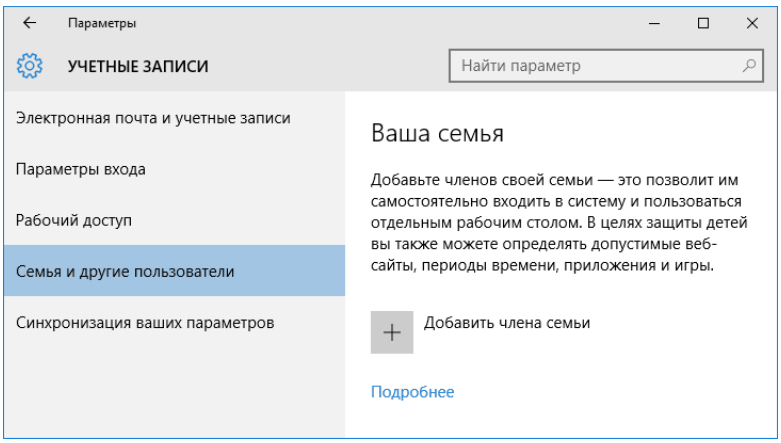

Рисунок – Екранна форма вікна облікового запису

Після входу в управління сімейними налаштуваннями ОС Windows 10 на сайті Microsoft можна побачити список облікових записів родини. Вибравши створений обліковий запис дитини, відкриється перелік основних напрямків керування.

Ще одним засобом захисту даних є шифрування даних певного диску, який доданий. Найвідоміша програма для шифрування даних диску на ПК із ОС Windows – BitLocker Anywhere. Для конролю ПЗ, що викоистовується а ПК застосовують технологію AppLocker (місцезнаходження технології проілюстровано на рисунку 3.3)

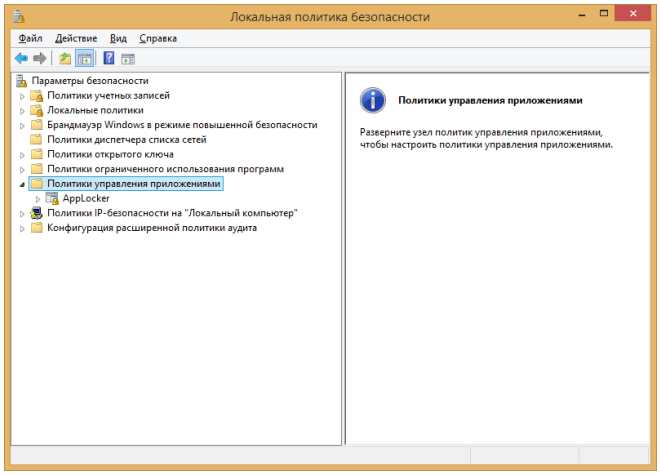

Рисунок 3.3 – Екранна форма вікна доступу до технології AppLocker

Крім цього існує можливість створення домашньої групи для доступу всіх домашніх ПК до інформації, що зберігається в домашній мережі. Домашня група – це функція, за допомогою якої будь-який користувач може

налаштувати загальний доступ до файлів або принтера в домашній мережі. Досить клацнути мишею, щоб отримати доступ до файлів і принтерів на інших комп'ютерах домашньої мережі. Наприклад, якщо потрібно надрукувати будь-який документ, переходити до іншого комп'ютера, до якого підключений принтер, не потрібно, а доступ до файлів, що зберігаються на домашньому комп'ютері, можна отримати і з іншого комп'ютера або ноутбука.

У процесі налаштування або приєднання до домашньої групи можна вибрати бібліотеки і принтери, які можна використовувати спільно, або з легкістю змінити їх у майбутньому. Домашню групу можна захистити паролем, який також можна змінити в будь-який час.

При цьому домашня мережа знаходиться під захистом, і проникнути в неї стороннім особам досить складно. Щоб додати комп'ютер в «Домашню групу» необхідно знати пароль, який автоматично генерується системою при першій активації функції «Домашня група».

Для установки домашньої групи необхідно мати домашню мережу. Домашня група – це середовище для забезпечення загального доступу до файлів і принтерів в існуючій мережі. Спочатку в центрі управління мережами і загальним доступом на панелі управління (див. рис. 3.4) потрібно перевірити, що для поточного мережевого розміщення встановлено параметр «Домашня мережа».

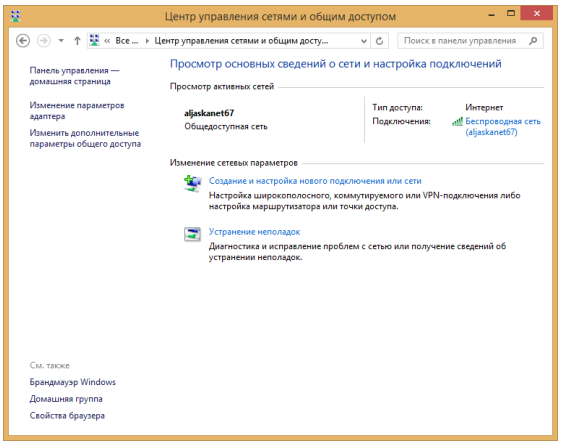

Рисунок 3.4 – Відкриття центру управління мережами і загальним доступом для визначення мережевого розміщення

Щоб змінити мережеве розміщення, досить просто клацнути на поточний параметр і вибрати будь-який інший (проте не слід встановлювати параметр «Домашня мережа» для публічної мережі, зазвичай, вона не є безпечною).

При установці ОС Windows на комп'ютері домашньої мережі домашня група буде налаштована автоматично. Навіть при підключенні робочого ноутбука (що знаходиться в корпоративному домені) до домашньої групи можна отримати загальний доступ до файлів і принтерів інших користувачів. Для доступу до домашньої групи застосовується єдиний пароль, що значно спрощує її створення і підключення до неї. Для того, щоб папки на цих комп'ютерах були доступні кожному з комп'ютерів, необхідно лише запустити майстер установки домашньої групи на одному з них.

Слід враховувати, що таке вікно з'явиться лише в тому випадку, якщо в мережі не створено жодної домашньої групи. В іншому випадку комп'ютер лише може приєднатися до існуючої групи, створення двох домашніх груп в одній підмережі неможливо.

Після створеня «Домашньо група», система запитає про те, до якого типу особистого вмісту користувач хоче надати користувачам спільний доступ в домашній групі. Після вибору відповідних папок для загального доступу система автоматично згенерує пароль для домашньої групи, і робота майстра налаштування буде завершено. Це не означає, що користувачі домашньої мережі будуть автоматично додані в домашню групу.

Наданий спочатку «Домашньою групою» пароль, можна змінити при потребі. Якщо змінити пароль домашньої групи, то при введенні його на одному комп'ютері він буде автоматично змінений на всіх інших комп'ютерах групи. Навіть якщо забути пароль для домашньої групи, то його можна подивитися на будь-якому комп'ютері, що входить в домашню групу. Для цього потрібно натиснути кнопку Пуск і перейти в Панель управління, набрати домашня група в поле для пошуку, клацнути елемент Домашня

група, а потім вибрати команду «Показати або роздрукувати» пароль домашньої групи.

Після успішного приєднання до домашньої групи у кожного з комп'ютерів в провіднику з'явиться рядок «Комп'ютери домашньої групи». У ній будуть знаходитися комп'ютери, що входять у віртуальну мережу.

При натисканні на обраному комп'ютері користувач отримає доступ до папок, які дозволені для загального доступу налаштуваннями цього комп'ютера.

При виникненні проблем, пов'язаних з домашньою групою, для їх вирішення можна скористатися засобом усунення проблем. Також у центрі підтримки Windows можна знайти додаткові відомості щодо усунення проблем, які можуть виникнути при використанні домашньої групи.

Хід роботи

1. Дослідити можливості адміністрування ОС Windows.
2. Дослідити функцію «Батьківський контроль» ОС Windows.
3. Зашифрувати диск за допомогою BitLocker ОС Windows.
4. Дослідити технологію AppLocker ОС Windows.
5. Проаналізувати засоби блокування мережевих загроз.
6. Усі проведені дослідження оформити у звіт про виконання лабораторної роботи.

Контрольні запитання

1. Можливості адміністрування в ОС Windows.
2. Які можливості «батьківського контролю» в ОС Windows?
3. Яка мінімальна кількість символів повинна бути в паролі для надійного захисту інформації?
4. Для чого застосовується BitLocker?
5. Як здійснюється шифрування у ОС Windows засобами BitLocker?
6. Які особливості застосування AppLocker в ОС Windows?

ЛАБОРАТОРНА РОБОТА 4
ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ АНТИВІРУСНИХ ПРОГРАМ

Мета: ознайомитися з програмними засобами захисту комп'ютерних систем від вірусів.

Теоретичні віомості

Відомі програмні віруси можна класифікувати за такими ознаками:

- середовище існування;
- способм зараження довкілля;
- впливом;
- особливостями алгоритму.

У залежності від середовища перебування віруси можна розділити на:

- мережеві;
- файлові;
- завантажувальні;
- файлово-завантажувальні.

Мережні віруси поширюються по різних комп'ютерних мереж.

Файлові віруси впроваджуються головним чином у виконавчі модулі, тобто у файли, що мають розширення COM та EXE. Вони можуть впроваджуватися й в інші типи файлів, але, як правило, записані в таких файлах, вони ніколи не одержують управління і, отже, втрачають здатність до розмноження.

Завантажувальні віруси впроваджуються в завантажувальний сектор диска (Boot-сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record).

Файлово-завантажувальні віруси заражають як файли, так і завантажувальні сектори дисків.

За способом зараження віруси поділяються на:

- резидентні;
- нерезидентні.

Резидентний вірус при зараженні (інфікуванні) комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження (файлів, завантажувальних секторів дисків і т. п.) і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до вимикання або перезавантаження комп'ютера.

Нерезидентні віруси не заражають пам'ять комп'ютера і є активними обмежений час.

За ступенем впливу віруси можна розділити на такі види:

- безпечні, не заважають роботі комп'ютера, але зменшують обсяг вільної оперативної пам'яті і пам'яті на дисках, дії таких вірусів виявляються в яких-небудь графічних або звукових ефектах;
- небезпечні віруси, які можуть призвести до різних порушень в роботі комп'ютера;
- дуже небезпечні, вплив яких може призвести до втрати програм, знищення даних, стирання інформації в системних областях диска.

За особливостями алгоритму віруси важко класифікувати через велику їх різноманітність. Найпростіші віруси – паразитичні, вони змінюють вміст файлів і секторів диска і можуть бути досить легко виявлені і знищені. Віруси-станції, звані хробаками, які поширюються по комп'ютерних мережах, обчислюють адреси мережних комп'ютерів і записують за цими адресами свої копії.

Віруси-невидимки, звані стелс-вірусами, які дуже важко виявити і знешкодити, так як вони перехоплюють звертання операційної системи до уражених файлів і секторів дисків і підставляють замість свого тіла незаражені ділянки диска. Найбільш важко знайти віруси-мутанти (поліморфні віруси), що містять алгоритми шифрування-розшифрування, завдяки яким копії одного і того ж вірусу не мають ні одного повторюваного ланцюжка байтів. Є й так звані квазівірусні або «троянські» програми, які хоч

і не здатні до самопоширення, але дуже небезпечні, тому що, маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків.

Способи протидії комп'ютерним вірусам можна розділити на кілька груп:

- профілактика вірусного зараження і зменшення можливої шкоди від такого зараження;
- методика використання антивірусних програм, в тому числі знешкодження і видалення відомого вірусу;
- способи виявлення і видалення невідомого вірусу.

Для виявлення, видалення і захисту від комп'ютерних вірусів розроблені спеціальні програми, які дозволяють виявляти і знищувати віруси. Такі програми називаються антивірусними. Сучасні антивірусні програми являють собою багатофункціональні продукти, що поєднують як превентивні, профілактичні засоби, так і засоби лікування вірусів і відновлення даних.

Вимоги до антивірусних програм наступні.

1) Стабільність і надійність роботи.

2) Розміри вірусної бази програми (кількість вірусів, які правильно визначаються програмою). З урахуванням постійної появи нових вірусів база даних повинна регулярно оновлюватися. Сюди ж слід віднести і можливість програми визначати різноманітні типи вірусів, і вміння працювати з файлами різних типів (архіви, документи). Важливим також є наявність резидентного монітора, що здійснює перевірку всіх нових файлів в режимі реального часу (тобто автоматично).

3) Швидкість роботи програми, наявність додаткових можливостей типу алгоритмів визначення навіть невідомих програмі вірусів (евристичне сканування). Сюди ж слід віднести можливість відновлювати заражені файли, не стираючи їх з жорсткого диска, а лише видаливши з них віруси.

Важливим є також відсоток помилкових спрацьовувань програми (помилкове визначення вірусу в "чистому" файлі).

4) Багатоплатформність (наявність версій програми під різні операційні системи).

Найпопулярніші та ефективні види антивірусних програм.

1. **Антивірусні сканери.** Принцип роботи антивірусних сканерів заснований на перевірці файлів, секторів і системної пам'яті та пошуку в них відомих і нових (невідомих сканеру) вірусів. Для пошуку відомих вірусів використовуються так звані маски. Маскою віруса є деяка постійна послідовність коду, специфічна для цього конкретного вірусу. Якщо вірус не містить постійної маски або її довжина недостатньо велика, то використовуються інші методи. До переваг сканерів відноситься їх універсальність, до недоліків – розміри антивірусних баз, які сканерам доводиться переносити за собою, і відносно невелика швидкість пошуку вірусів.

2. **CRC-сканери** (програми-ревізори). Принцип роботи CRC-сканерів заснований на підрахунку CRC-сум (контрольних сум) для присутніх на диску файлів системних секторів. Ці CRC-суми потім зберігаються в БД антивіруса. При наступному запуску CRC-сканери звіряють дані, що містяться в БД, з реально підрахованими значеннями. Якщо інформація про фото, записана в БД, не збігається з реальними значеннями, то CRC-сканери сигналізують про те, що файл був змінений або заражений вірусом.

3. **Монітори** (або програми сторожі). Антивірусні монітори – це резидентні програми, що перехоплюють вірусонебезпечні ситуації і повідомляють про це користувачеві. До вірусонебезпечних відносяться виклики на відкриття для запису і виконання файли, запис у завантажувальні сектори дисків або MBR вінчестера, спроби програм залишитися резидентно і т.д., тобто виклики, які характерні для вірусів в моменти їхнього розмноження. До переваг моніторів належить їх здатність виявляти і

блокувати вірус на ранній стадії його розмноження, що, до речі, буває дуже корисно у випадках, коли відомий вірус постійно з'являється.

До недоліків відноситься існування шляхів обходу захисту монітора і велика кількість помилкових спрацьовувань, що, мабуть, і стало причиною для практично повної відмови користувачів від подібного роду антивірусних програм. Існує кілька більш універсальних апаратних моніторів, але до перерахованих вище недоліків додаються також проблеми сумісності зі стандартними конфігураціями комп'ютерів і складнощі при їх встановлення та налаштування. Все це робить апаратні монітори вкрай непопулярними поряд з іншими типами антивірусного захисту.

4. **Іммунізатори** (або програми вакцини). Іммунізатори поділяють на два типи: іммунізатори, що повідомляють про зараження, та іммунізатори, що блокують зараження яким-небудь типом вірусу. Перші, зазвичай, записуються в кінець файлів і при запуску файлу кожного разу перевіряють його на зміну.

Другий тип імунізації захищає систему від зараження вірусом якого-небудь виду. Файли на дисках модифікуються таким чином, що вірус приймає їх за вже заражені. Для захисту від резидентного вірусу в пам'ять комп'ютера заноситься програма, що імітує копію вірусу, при запуску вірус натикає на неї і вважає, що система вже заражена.

5. **Програми-лікарі** (фаги). Програми-лікарі не тільки знаходять заражені вірусами файли, але і «лікують» їх, тобто видаляють із файлу тіло програми вірусу, повертаючи файли в початковий стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх, і тільки потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку і знищення великої кількості вірусів.

6. **Програми-детектори.** Програми-детектори забезпечують пошук і виявлення вірусів в оперативній пам'яті, на зовнішніх носіях. Розрізняють детектори універсальні і спеціалізовані. Універсальні детектори в своїй роботі використовують перевірку незмінності файлів шляхом підрахунку та

порівняння з еталоном контрольної суми. Недолік універсальних детекторів пов'язаний з неможливістю визначення причин викривлення файлів. Спеціалізовані детектори здійснюють пошук відомих вірусів по їх сигнатурі (повторюваній ділянці коду). Недолік таких детекторів полягає в тому, що вони не здатні виявляти всі відомі віруси.

Хід роботи

1. Дослідити антивірусну програму, що встановлена на робочому ПК, визначити статус захисту.
2. Ознайомитись з інтерфейсом антивірусної програми, режимами роботи, модулями, основними можливостями (здійснити перевірку комп’ютера та зовнішнього пристрою на наявність вірусів), способами оновлення антивірусної бази, режими захисту комп’ютера у мережі.
3. Дослідити захист інформації за допомогою фаєрволу (брандмауєра) ОС Windows.
4. Дослідити стан захисту ОС для таких випадків:

a) без увімкнутого брандмауера,

b) використовуючи вбудований в ОС брандмауер;

c) встановити інший вільно обраний брандмауер (таблиця 4.1 згідно варіанту).

Таблиця 4.1. – Список фаєрволів

Варіант	Фаєрвол
1	Online Armor Free
2	Comodo Firewall 2012
3	Outpost Firewall Free
4	ZoneAlarm Free Firewall
5	PC Tools Firewall Plus

6 Sunbelt Personal Firewall

7 Outpost Security Suite Free

8 GeSWall

9 Windows 7 Firewall Control

10 Webroot Desktop Firewall

11 FortGuard Firewall Free Edition

12 Doors Firewall

13 AGAVA Firewall

14 Ashampoo Firewall Free

15 Privatefirewall

16 RusRoute

17 Rising Personal Firewall

18 AVS Firewall

19 Windows Firewall Control

20 DefenseWall Personal Firewall

21 FortKnox Personal Firewall

22 Jetico Personal Firewall

23 TinyWall

24 SpyShelter Firewall

5. Описати принцип роботи і політики безпеки обраного брандмауера.

6. Навести приклади журналу фільтрації мережевого трафіку.

7. Для визначення ефективності кожного брандмауера скористатися сканером безпеки.

8. Визначити можливості та недоліки фаєрволу, що використовується.

9. Усі отримані результати оформити у вигляді звіту про виконання лабораторної роботи, використовуючи скріншоти для ілюстрації здійсненої роботи.

Контрольні запитання

1. Що таке вірус?
2. Які основні типи вірусів?
3. Що таке антивірусна програма?
4. Які основні вимоги до антивірусних програм?
5. Які типи антивірусних програм існують на даний час?
6. Що таке фаєрвол? Для чого він призначений? Які його основні характеристики?

ЛАБОРАТОРНА РОБОТА №5
РОЗРОБКА ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Мета: засвоїти методику та отримати практичні навики побудови засобів ідентифікації користувачів.

Теоретичні відомості

Ідентифікація об'єкта – це одна з функцій підсистеми захисту. Перед тим, як отримати доступ до комп'ютерної системи, користувач повинен ідентифікувати себе, після чого засоби захисту повинні підтвердити, чи такий користувач є насправді тим, за кого себе видає. Програма ідентифікації

призначена для однозначного встановлення особи користувача та надання йому прав доступу в систему. Одним з найпростіших способів ідентифікації є парольна ідентифікація, яка здійснюється шляхом порівняння введеного імені та паролю, із тими які зберігаються у файлі паролів (див.рис.5.1).

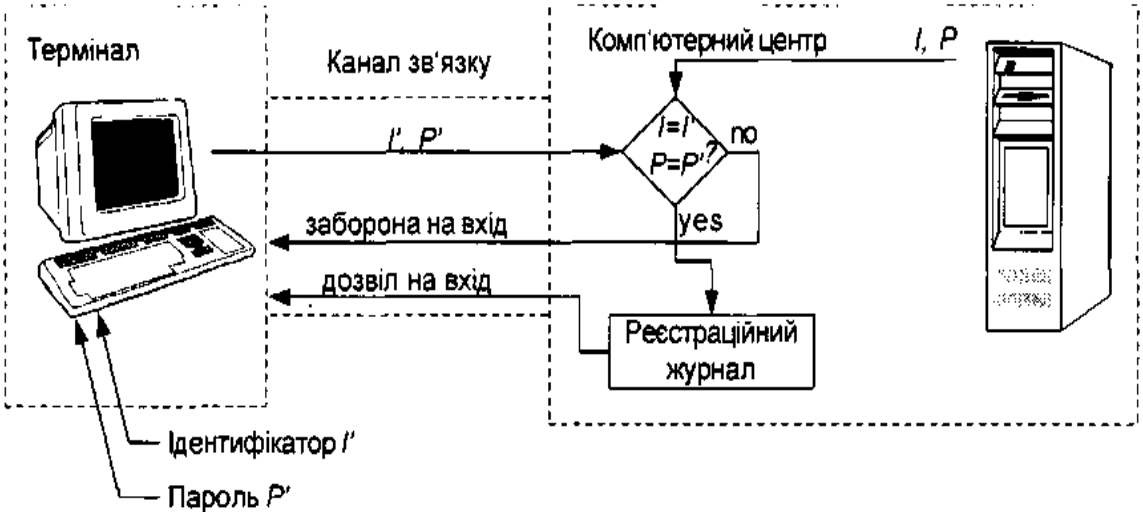

Рисунок 5.1 – Класичний спосіб парольної ідентифікації

Проте такий підхід, не захищає КС від програмних та апаратних засобів сканування клавіатури та ліній передачі, а отже може призвести до витоку конфіденційної інформації. Тому, як правило, в сучасних КС пароль не передається в явній формі по лініях передачі, а натомість в якості паролю використовують якесь його відображення. У якості такого відображення використовуються важкооборотні однонапрямлені функції, застосування яких гарантує неможливість розкриття пароля за його відображенням за розумний час.

В такому випадку процедура ідентифікації описується таким алгоритмом (див. рис.5.2):

1) користувач вводить свій ідентифікатор;

2) засоби ідентифікації переглядають список зареєстрованих ідентифікаторів. Якщо ідентифікатор не зареєстрований, – то виводиться повідомлення, що такий користувач в системі не зареєстрований, і далі перехід на крок 1, або ж завершення роботи програми входу в систему. Якщо ж ідентифікатор зареєстрований, – то перехід на крок 3.

3) КС генерує випадкове число x, та обчислює значення важкооборотної однонапрямленої функції y, яка використовується в системі для відображення паролю користувача;

4) число x передається користувачу;

5) користувач обчислює значення важкооборотної однонапрямленої функції y та передає його в КС;

6) КС порівнює значення y та y'. Якщо вони співпадають, то КС дозволяє вхід користувача в систему. В інакшому випадку видається повідомлення про помилку вводу паролю, перехід на крок 3, або ж завершення роботи програми входу в систему.

Зрозуміло, що стійкість такої КС до інтерполяції використовуваної функції визначається важкооборотністю функції y та частотою генерації і розподілу ключів в системі.

Іншою важливою складовою частиною КС є програма реєстрації, яка призначена для реєстрації або видалення користувачів в Реєстраційному журналі системи із наданням їм певних прав доступу. Право реєстрації або видалення належить лише одному користувачу – адміністратору системи. Імена користувачів, їх паролі та права доступу зберігаються в явному вигляді у файлі. Розробник повинен оцінити розмір реєстраційного журналу, виходячи із заданих параметрів.

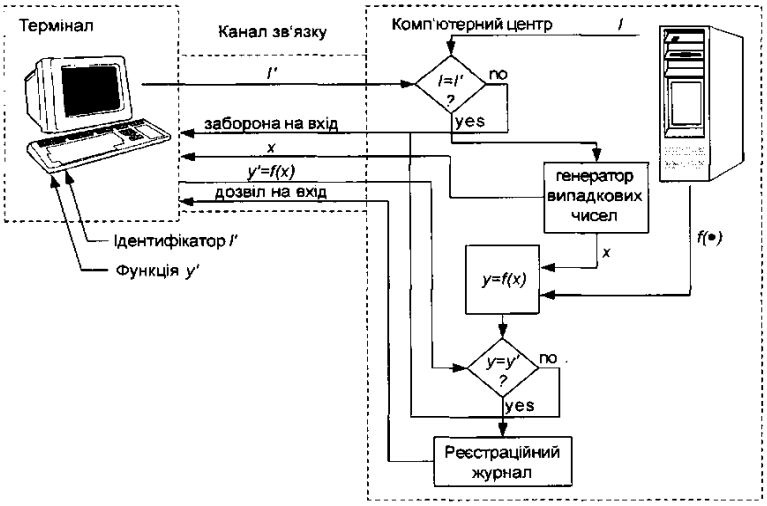

Рисунок 5.2 – Ідентифікація користувача за допомогою важкооборотної функції відображення паролю

Така інформація буде корисною для оцінки трудомісткості процедур сортування та фільтрування. Окрім того, на основі отриманих даних розробник може давати рекомендації адміністратору КС стосовно регулярності процедур генерування та розподілу ключів.

Хід роботи

1. Ознайомитись із теоретичними відомостями.
2. Отримати індивідуальне завдання у викладача.
3. Визначити функції системи.
4. Відповідно до індивідуального завдання розробити структуру заданої КС.
5. Провести розрахунки параметрів системи.
6. Розробити необхідне алгоритмічне забезпечення.
7. Реалізувати задану КС.
8. Оцінити розмір реєстраційного журналу.
9. Дати відповідь на контрольні запитання.
10. Скласти звіт із виконання лабораторної роботи.

Контрольні запитання

1. Що таке ідентифікація користувачів в КС?
2. Які види ідентифікації відомі?
3. Що таке парольна ідентифікація?
4. Які недоліки класичного способу парольної ідентифікації?
5. Що таке реєстраційний журнал?
6. Для чого використовують реєстраційні журнали?
7. Як оцінити об’єм реєстраційного журналу?

Структура звіту

1. Назва та зміст лабораторної роботи.
2. Структурна схема та параметри розробленої КС.

3. Розрахунок розміру реєстраційного журналу.

4. Текст програми основних модулів КС.

5. Реєстраційний журнал.

6. Висновки.

Індивідуальні завдання

Розробити програму ідентифікації користувачів, котра б фіксувала вхід (вихід) користувачів в Реєстраційному журналі. Необхідні параметри програми наведені в таблиці 5.1.

Таблиця 5.1 – Список параметрів програми

Варіант	Кількість користувачів	Кількість рівнів доступу	Кількість реалізованих функцій	Функція криптування пароля
1.	5	2	>5	*exp(-a*x)*
2.	6	3	>5	*lg(a*x)*
3.	7	4	>5	*a*sin(x)*
4.	8	2	>5	*a*ln(x)*
5.	9	3	>5	*a/x*
6.	10	4	>5	*Iд(a/x)*
7.	11	2	>5	*x/sin(a)*
8.	12	3	>5	*a*sin(1/x)*
9.	14	4	>5	*tg(a*x)*
10.	16	2	>5	*a*ln(2 + x)*

ЛАБОРАТОРНА РОБОТА №6
РОЗРОБКА ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Мета: засвоїти методику та отримати практичні навики побудови засобів аутентифікації користувачів.

Теоретичні відомості

Аутентифікація полягає в періодичній (стохастичній) перевірці достовірності ідентифікації користувача. Така процедура проводиться для повторної перевірки користувача. Аутентифікація може здійснюватись як апаратними, так і програмними методами за якимись особистими ознаками чи персональними відомостями користувача.

При апаратній реалізації користувач може бути аутентифікованим за певними фізичними ознаками: вага тіла, колір очей, відбитки пальців, геометрія долоні, код ДНК і т.п. Окрім того, можуть використовуватись додаткові особисті пристрої: наручні браслети, ключі і т.д. Такий вид аутентифікації характеризується вищим рівнем надійності, проте є складнішим та дорожчим у використанні, тому він використовується на підприємствах, де необхідно забезпечити високий рівень захисту інформації.

Дешевший варіант аутентифікації користувачів полягає у створенні програмних засобів. Резидентна програма періодично з певним кроком часу задає випадковим чином запитання із заздалегідь створеного файлу, або ж випадкові три- , чотири- розрядні десяткові числа. КС порівнює відповіді з наперед зареєстрованими, або ж обчисленими відповідями, і на основі цього надає, або забороняє роботу користувача. У випадку правильної відповіді за користувачем залишаються його права, а у випадку неправильної відповіді – користувач втрачає права доступу і повинен заново ввійти в систему. Стійкість такого виду аутентифікації забезпечується конфіденційністю інформації.

Основні способи аутентифікації користувачів:

- наперед визначена інформація, якою може користуватися користувач: пароль, персональний ідентифікаційний номер, домовленість про використання спеціальних закодованих фраз;
- елементи апаратного забезпечення, якими може користуватися користувач: ключі, магнітні карточки, мікросхеми і т.п.;

- характерні особисті ознаки користувача: відбитки пальців, рисунок сітківки ока, тембр голосу і т.п.;
- характерні навики та риси поведінки користувача в режимі реального часу: особливості динаміки та стиль роботи на клавіатурі, прийоми роботи з маніпулятором і т.п.;
- навики та знання користувачів, обумовлені освітою, культурою, навчанням, вихованням, звичками і т.п.

Процедура аутентифікації користувачів може бути реалізована як з постійним, так і з адаптивним періодом повтору. Постійний період повтору використовується в тих КС, в яких частота появи користувачів в системі та інтенсивність їх роботи є приблизно рівномірною. При виборі періоду процедури аутентифікації слід керуватися такими міркуваннями: при досить великому періоді збільшується імовірність НСД, а при досить малому – зменшується ефективність роботи користувачів, оскільки вони постійно відволікаються від виконання основних своїх обов'язків. В системах, до яких ставляться вимоги підвищеної захищеності можуть застосовуватися засоби аутентифікації з адаптивним періодом повтору. Період повтору в таких КС визначається як інтенсивністю роботи користувачів, так і спробами НСД.

Окрім того, після встановлення достовірності ідентифікації користувача виконується реєстрація в часі всіх дій користувача в Операційному журналі системи. В такому журналі окрім записів санкціонованого використання тих, чи інших ресурсів системи, можуть накопичуватися дані про спроби несанкціонованого доступу користувачів з автоматичною сигналізацією адміністратору системи для прийняття організаційних заходів з метою виявлення порушників. При створенні операційного журналу слід пам'ятати, що різні типи користувачів мають доступ до різних типів ресурсів.

Для періодичної аутентифікації зручно використовувати переривання системного таймера INT 1Ch. Слід пам'ятати, що програма аутентифікації повинна заборонити усі інші види переривань.

INT 10h використовується для тимчасового очищення екрану шляхом використання функцій прокрутки чи перемиканням на іншу відео-сторінку.

INT 1Ап використовується для отримання точних значень системної дати та часу.

При побудові прикладних програмних засобів під Windows, краще використовувати компоненти типу TTimer.

Загальна структура КС аутентифікації приведена на рис. 6.1.

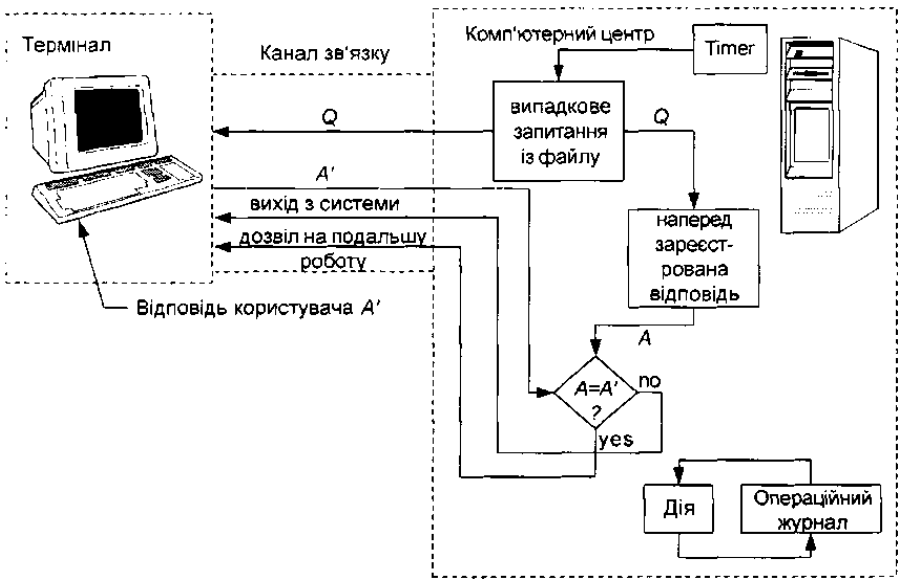

Рисунок 6.1 – Загальна структура КС аутентифікації

Хід роботи

1. Ознайомитись із теоретичними відомостями.
2. Отримати індивідуальне завдання у викладача.
3. Визначити функції системи.
4. Відповідно до індивідуального завдання розробити структуру заданої КС.
5. Провести розрахунки параметрів системи.
6. Розробити необхідне алгоритмічне забезпечення.
7. Реалізувати задану КС.
8. Оцінити розмір операційного журналу.
9. Скласти звіт із виконання лабораторної роботи

Контрольні запитання

1. Що таке аутентифікація користувачів в КС?
2. Які є види аутентифікації?
3. Назвіть основні способи аутентифікації користувачів в КС за допомогою програмних засобів.
4. Назвіть основні способи аутентифікації користувачів в КС за допомогою апаратних засобів.
5. Що таке операційний журнал?
6. Для чого використовують операційні журнали?
7. Як оцінити об’єм операційного журналу?

Структура звіту

1. Назва та зміст лабораторної роботи.
2. Відповідь на контрольні запитання.
3. Структурна схема та параметри розробленої КС.
4. Розрахунок розміру операційного журналу.
5. Текст програми основних модулів КС.
6. Операційний журнал.
7. Висновки.

Індивідуальні завдання

Розробити програму аутентифікації користувачів, котра б фіксувала дії користувачів в Операційному журналі. Необхідні параметри програми наведено в таблиці 6.1.

Таблиця 6.1 – Параметри програми

Варіант	Кількість рівнів доступу	Кількість запитань	Період повтору процедури аутентифікації, хв.	Кількість запитань в одній ітерації процедури аутентифікації
1.	2	15	2	3
2.	3	10	3	4

3.	4	20	4	2
4.	2	15	5	3
5.	3	15	6	4
6.	4	10	5	2
7.	2	20	4	3
8.	3	15	2	4
9.	4	10	3	2
10.	2	20	6	3

СПИСОК ЛІТЕРАТУРИ

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах. К.: КМ Академія, 2006. 244 с.
2. Бродо В.Л. Обчислювальні системи, мережі та телекомунікації: Підручник для вузів. 2-ге видання М.: «Альянс-Прес», 2004 р. 495 с.
3. Вакалюк Т.А. Захист інформації в комп’ютерних системах. Навчально-методичний посібник.Житомир: Вид-во ЖДУ, 2013.136 с.
4. Вербіцький О. В. Вступ до криптографії. Видавництво НТЛ, Львів, 1998. 248 с.
5. Гримів С.С Локальні мережі: структура і робота.Спб.: БХВ-Пітер, 2004. 432с.
6. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. К.: Корнійчук, 2008. 152 с.
7. Косарєв В.П., Єрьомін Л.В. Комп'ютерні системи та мережі. М.: Фінанси і статистика, 2001. 590 с.
8. Молдовян А. А., Молдовян В. А., Советов В. Я. Криптография. Серия “Учебники для вузов. Специальная литература”. СПБ: Издательство “Лань”, 2000. 224 с.

9. Молдовян Н. А., Зима В. М. Введение в практическую криптографию. Учебное пособие. Санкт-Петербург: Военный инженерно-космический университет имени А. Ф. Можайского, 2001. 280 с.

10. Романець Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999. 328 с.

11. Столлингс В. Криптография и защита сетей: принципы и практика. 2-е изд. М.: Изд. дом “Вильямс”,2001. 672 с.

12. Фурман О.М. Мережеві можливості MS Windows. М.: Перспектива, 2006. 385 с.

13. Шаньгин В. Ф. Информационная безопасность и защита информации. М.: ДМК Пресс, 2016. 702 с.

14. Широчин В. П., Мухин В. В., Кулик А. В. Вопросы и проектирования механизмов защиты информации в компьютерных системах и сетях. К.: “ВЕК+”, 2000. 112 с.