

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА ІНФОРМАТИКИ І КОМП'ЮТЕРНИХ НАУК

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАПОБІГАННЯ
ВИТОКУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Виконав: студент 2 курсу
другого (магістерського) рівня вищої освіти
спеціальності 126 «Інформаційні системи та технології»
ОПП «Інформаційні системи та технології»
Шумков С.О.

Керівник: Григорова А.А.

Рецензент: Захарченко Р.М.
(прізвище та ініціали)

Хмельницький – 2024 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

(повне найменування вищого навчального закладу)

Факультет інформаційних технологій та дизайну

Кафедра Інформатики і комп'ютерних наук

Рівень вищої освіти другий (магістерський)

Спеціальність 126 «Інформаційні системи та технології»

Освітньо-професійна програма «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедру В.І. Литвиненко

«___» _____ 2023 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Шумкову Сергію Олеговичу

(прізвище, ім'я, по батькові)

1. Тема роботи Розробка програмного забезпечення запобігання витоку інформації на підприємстві

керівник роботи Григорова Анжела Анатоліївна, к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «29» вересня 2023 року № 507-с

2. Строк подання студентом роботи 11 грудня 2023 р.

3. Вихідні дані до роботи нормативна та статистична документація, методичні рекомендації до виконання, оформлення та захисту кваліфікаційної роботи магістра для студентів всіх форм навчання за спеціальністю 126 «Інформаційні системи та технології»

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Програмне забезпечення інформаційної безпеки

2. Порівняльний аналіз технологій захисту

3. Комплексне керування системою безпеки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	Григорова А.А.	11.09.2023	01.2024

7. Дата видачі завдання 11.09.2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи магістра	Строк виконання етапів роботи	Примітка
1.	Огляд літературних джерел з теми	вересень 2023	виконано
2.	Складання і затвердження плану роботи	вересень 2023	виконано
3.	Написання 1 розділу	вересень-жовтень 2023	виконано
4.	Написання 2 розділу	жовтень 2023	виконано
5.	Написання 3 розділу	листопад 2023	виконано
7.	Формулювання висновків за темою дослідження	листопад 2023	виконано
8.	Оформлення роботи	листопад 2023	виконано
9.	Надання роботи керівнику для перевірки та написання подання	листопад 2023	виконано
10.	Подання роботи на рецензування	листопад 2023	виконано
11.	Подання роботи для перевірки у КСПНП	грудень 2023	виконано
12.	Захист роботи в ЕК	грудень 2023	виконано

Студент _____ Шумков С.О.
(підпис)Керівник роботи _____ Григорова А.А.
(підпис)

РЕФЕРАТ

Кваліфікаційна робота магістра містить 67 сторінок, 4 таблиці, 14 рисунків, список літератури з 18 найменувань, 1 додаток.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

У першому розділі роботи розглядається поняття та сутність основних факторів захисту, переваги та недоліки міжмережевого екрану, брандмауера Windows Defender, різниця між Proxy та VPN.

У другому розділі представлений аналіз антивірусних програм для безпеки програмного забезпечення підприємства.

У третьому розділі розглядається програмний продукт для управління Active Directory, здійснюється налаштування політики Active Directory, згідно з яким формується доступ та захист користувачів у комп'ютерній мережі.

КЛЮЧОВІ СЛОВА: ACTIVE DIRECTORY, PROXY, VPN, WINDOWS DEFENDER, ЗАХИСТ ІНФОРМАЦІЇ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ЗМІСТ

Список умовних скорочень.....	6
Вступ.....	7
Розділ 1. Програмне забезпечення інформаційної безпеки	9
1.1. Інформаційна безпека підприємства	9
1.2. Основні фактори захисту	14
1.3. Міжмережевий екран	15
1.4. Active Directory, Proxy, VPN.....	21
Розділ 2. Порівняльний аналіз технологій захисту.....	29
2.1 Антивірус Norton.....	29
2.2. Антивірус TotalAV	31
2.3. Антивірус McAfee	32
2.4. Антивірус Intego	34
2.5. Антивірус Bitdefender.....	35
2.6. Антивірус Panda Dome.....	36
2.7. Антивірус Avira	37
2.8. Порівняння антивірусів.....	39
2.9. Порівняння VPN сервісів.....	41
2.10. Порівняння VPN-протоколів.....	44
Розділ 3. Комплексне керування системою безпекою	46
3.1. Служби захисту інформації, її структура та функції.....	46
3.2. Система Active Directory	48
3.3. Середовище розробки програмного забезпечення.....	54
3.4. Розробка програмного забезпечення	59
Висновок	62
Список використаних джерел	63
Додаток А.....	65

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ	- Комплексна система захисту інформації
КС	- Комп'ютерна система
НСД	- Несанкціонований доступ
VPN	- Virtual private network
TCP	- Transmission Control Protocol
ПЗ	- Програмне забезпечення
RAM	- Random Access Memory
DNS	- Domain Name System

ВСТУП

Актуальність дослідження. Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами. З кожним роком з розвитком комерційної та підприємницької діяльності збільшується число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації знаходяться в центрі уваги багатьох спеціалістів. Зростає потреба у фахівцях із захисту інформації та відповідному програмному забезпеченню.

Захист інформації від витоку технічними каналами - це комплекс організаційних, організаційно-технічних і технічних заходів, що виключають або послаблюють безконтрольний вихід конфіденційної інформації за межі контрольованої зони.

Причини витоку інформації пов'язані, з недосконалістю норм щодо збереження інформації, а також порушенням цих норм, відступом від правил поведіння з технічними засобами, та іншими матеріалами, що містять конфіденційну інформацію.

На будь-якому підприємстві постає питання побудови комплексної системи захисту інформації, але особливу увагу слід приділити захисту від витоку інформації технічними каналами витоку інформації.

Подолання витоку інформації на підприємстві дає можливість продовжити життєдіяльність підприємства, забезпечити його відродження на тому ж або більш високому рівні.

Об'єкт дослідження – технології забезпечення захисту інформації.

Предмет дослідження – методи реалізації ефективної системи безпеки захисту інформації.

Метою роботи є розробка програмного забезпечення для комплексного керування системи безпеки та захисту від витоку інформації на підприємстві.

Задачами дослідження є:

- вивчення теоретичних основ витоку інформації та основних факторів захисту комп'ютерних систем;
- аналіз антивірусних програм для комп'ютерних систем;
- діагностика сильних та слабких сторін захисту інформації;
- опис основних напрямів подолання витоку інформації з комп'ютерних систем на підприємстві;
- розробка програмного забезпечення.

Дана кваліфікаційна робота складається зі вступу, трьох розділів, висновку, одного додатку та списку використаних джерел.

У першому розділі роботи розглядається поняття та сутність програмних засобів захисту інформації; поняття брандмауера та його переваги і недоліки; особливості проксі-сервера та VPN-сервісів.

У другому розділі представлений порівняльний аналіз антивірусних програм для комп'ютерних систем, та порівняння vpn-протоколів.

У третьому розділі розглядається програмний продукт для управління Active Directory, здійснюється налаштування політики Active Directory, згідно з яким формується доступ та захист користувачів у комп'ютерній мережі.

Чітка, комплексна та своєчасна діагностика стану підприємства – головний етап в розробці комплексного захисту витоку інформації з комп'ютерної системи підприємства.

За результатами проведеного дослідження опубліковано тези у матеріалах VI Всеукраїнської науково-практичної інтернет - конференції «Сучасні комп'ютерні системи та мережі в управлінні».