

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ЗАКЛАД
„ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА”

Навчально-науковий інститут фізики, математики та інформаційних
технологій

Кафедра інформаційних технологій та систем

Берест Ростислав Юрійович

**Розробка системи методів та засобів захисту даних в комп'ютерної
мережі підприємства**

Бакалаврська робота
за напрямом підготовки 123 Комп'ютерна інженерія

Особистий підпис – _____ Ростислав БЕРЕСТ

Науковий керівник – _____ асистент кафедри ІТС
(підпис) Володимир МАТІЄВСЬКИЙ
(посада, науковий ступінь,
наукове звання, ініціали, прізвище)

Зав. кафедри – _____ зав. кафедри ІТС, кандидат
(підпис) педагогічних наук, доцент,
Микола СЕМЕНОВ
(посада, науковий ступінь,
наукове звання, ініціали, прізвище)

Полтава – 2023

Міністерство освіти і науки України	
Державний заклад «Луганський національний університет імені Тараса Шевченка»	
Факультет (інститут)	Навчально-науковий інститут фізики, математики та інформаційних технологій <small>(повна назва)</small>
Кафедра	Інформаційних технологій та систем <small>(повна назва)</small>
Освітньо-кваліфікаційний рівень	Бакалавр <small>(код, назва)</small>
Напрямок підготовки	123 Комп'ютерна інженерія <small>(код, назва)</small>

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТС
М.А. Семенов

(підпис)

(ініціали, прізвище)

“ ” 2023 р.

**ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ**

Берест Ростислав Юрійович

(прізвище, ім'я, по батькові)

1. Тема роботи

**РОЗРОБКА СИСТЕМИ МЕТОДІВ ТА ЗАСОБІВ
ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРНОЇ
МЕРЕЖІ ПІДПРИЄМСТВА**

Керівник кваліфікаційної роботи

Матієвський В.В. асистент кафедри ІТС
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджена наказом по університету

від

2. Строк подання студентом проекту (роботи)

3. Вихідні дані до роботи (проекту)

(визначаються кількісні або (та) якісні показники, яким повинен відповідати об'єкт розробки)

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) **ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ**

**ОСНОВНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В
МЕРЕЖАХ**

**МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В
КОРПОРАТИВНИХ МЕРЕЖАХ**

(визначаються назви розділів або (та) перелік питань, які повинні увійти до тексту ПЗ)

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

6. Консультанти розділів проекту/роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання „_____” _____ 2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Вибір теми роботи, вивчення наукової літератури, затвердження теми та керівника.	До 1 листопада	
2.	Аналіз літературних джерел за темою роботи. Подання структури теоретичної частини роботи та плану експериментальних досліджень.	Другий тиждень листопада (10 листопада)	
3.	Робота над теоретичною частиною. Подання теоретичної частини роботи для першого читання науковим керівником.	До 15 грудня	
4.	Усунення зауважень, урахування рекомендацій наукового керівника. Подання теоретичної частини роботи на друге читання.	До 28 січня	
5.	Проведення експериментальної роботи. Поетапний аналіз та обговорення її результатів. Перевірка стану виконання роботи.	Перший тиждень березня	
6.	Урахування рекомендацій наукового керівника, усунення недоліків, підготовка варіанта роботи до передзахисту. Розробка презентації.	До 31 березня	
7.	Попередній захист роботи на кафедрі	травень	
8.	Доопрацювання роботи з урахуванням рекомендацій після передзахисту. Подання роботи науковому керівникові та рецензентові на підготовку відгуку та рецензії	За 10 днів до державної атестації	
9.	Подання на кафедру остаточного варіанта роботи, переплетеного та підписаного автором, науковим керівником і рецензентом.	За 5 днів до державної атестації	

Студент

підпис

Керівник проекту (роботи)

підпис

Р.Ю. Берест

(ініціали, прізвище)

В.В. Матієвський

(ініціали, прізвище)

АНОТАЦІЯ

Берест Р.Ю.

Тема: Розробка системи методів та засобів захисту даних в комп'ютерній мережі підприємства

Спеціальність: 123 «Комп'ютерна інженерія»

Установа: ЛНУ імені Тараса Шевченка, 2023 р.

Бакалаврська робота містить: 59 с., 3 рис., 14 джерел, 2 додатка.

Об'єктом дослідження є передача даних в корпоративних мережах.

Предметом дослідження є методи та засоби захисту інформації при передачі даних в корпоративних мережах.

Мета роботи - дослідити та розробити модель захисту та збереження інформації

Результати роботи.

Вивчено теоретичні відомості, щодо основних загроз, розглянуто класифікацію загроз безпеки, виділені найбільш поширені загрози, опрацьовано; основні методи та засоби захисту, фізичний захист інформації, апаратні та програмні засоби захисту інформації в корпоративних мережах. Захист інформації в корпоративній мережі, захист інформації від несанкціонованого доступу .

Висновки. Розроблено план заходів із захисту інформації в мережі підприємства. Основні методи захисту інформації в корпоративній мережі на основі Windows

Ключові слова: ВІРУС, ФІШИНГ, СПУФІНГ, DDOS, АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

ABSTRACT

Berest R.Yu.

Theme: Development of a system of methods and means of data protection in the computer network of the enterprise.

Speciality: 123 "Computer Engineering"

Institution: Luhansk Taras Shevchenko National University (LTSNU), 2023.

Bachelor's thesis contains: 59 pages, 3 figs., 14 sources, 2 appendices.

The object of research there is data transfer in corporate networks.

The subject of the study is methods and means of protecting information when transferring data in corporate networks.

The purpose of the work is explore and develop a model for protecting and storing information

Job performances. Theoretical information on the main threats was studied, the classification of security threats was considered, the most common threats were identified, worked out; basic methods and means of protection, physical protection of information, hardware and software for information protection in corporate networks. Protection of information in the corporate network, protection of information from unauthorized access

Conclusions. An action plan for the protection of information in the enterprise network has been developed. Basic methods of protecting information in a Windows-based corporate network.

Keywords. VIRUS, PHISHING, SPOOFING, DDOS, INFORMATION SECURITY HARDWARE, INFORMATION SECURITY SOFTWARE

ТС.4КІ.0723.01-ВП

ВІДОМІСТЬ ПРОЕКТУ. РОЗРОБКА ПРИСТРОЮ ДЛЯ РОЗУМНОГО БУДИНКУ НА БАЗІ МАІХDUINO

[illegible]

					ІТС.4КІ.0721.01-ВП					
Змн.	Арк.	№ докум.	Підпис	Дата	ВІДОМІСТЬ ПРОЕКТУ			Лім.	Арк.	Акрушів
Розроб.		Берест Р.Ю.								
Керівник		Матієвський В.В.							1	1
Реценз.		Козуб Ю.Г.						ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.										
Зав. каф.		Семенов М.А..								

Міністерство освіти і науки України
Державний заклад «Луганський національний університет
імені Тараса Шевченка»

Факультет (інститут)

Навчально-науковий інститут фізики,
математики та інформаційних технологій

(повна назва)

Кафедра

Інформаційних технологій та систем

(повна назва)

(код, назва)

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання програмної розробки (ПР):

РОЗРОБКА СИСТЕМИ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ В
КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

ІТС.4КІ.0723.02-ТЗ

ПОГОДЖЕНО

Керівник кваліфікаційної роботи

_____ Матієвський В.В. _____

“ _____ ” _____ 2023р

ВИКОНАВЕЦЬ

Студент групи 4 КІ

_____ Берест Р.Ю. _____

“ _____ ” _____ 2023р

Полтава – 2023

ЗМІСТ

ВСТУП.....	3
1. ХАРАКТЕРИСТИКИ МЕРЕЖІ	3
2. ПРИЗНАЧЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ.....	3
3. ОСНОВНІ ВИМОГИ ДО МЕРЕЖІ.....	3
4. ТЕХНІКО-ЕКОНОМІЧНІ ВИМОГИ ДО КІНЦЕВОГО ПРИСТРОЮ .	4
6. ЕТАПИ ВИКОНАННЯ ПР	4
7. ПОРЯДОК ВНЕСЕННЯ ЗМІН ДО ТЕХНІЧНОГО ЗАВДАННЯ, ЩО ЗАТВЕРДЖЕНО.....	4

					ІТС.4КІ.0723.02-ТЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	ТЕХНІЧНЕ ЗАВДАННЯ			Лім.	Арк.	Акрушів
Розроб.		Берест Р.Ю.								
Керівник		Матієвський В.В.							2	7
Реценз.		Козуб Ю.Г.						ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.										
Зав. каф.		Семенов М.А..								

ВСТУП

- 1.1 Найменування: Розробка системи методів та засобів захисту даних в комп'ютерної мережі підприємства
- 1.2 Шифр ПР: ІТС.4КІ.0723
- 1.3 Підстава для виконання ПР: Підставою для виконання даної розробки є завдання на виконання дипломного проекту, яке затверджено кафедрою інформаційних технологій та систем Луганського національного університету імені Тараса Шевченка.
- 1.4 Терміни розробки:
- 1.4.1 Початок 11 листопада 2022р.
- 1.4.2 Закінчення 15 травня 2023р.
- 1.5 Фінансується за рахунок коштів замовника. Умови фінансування - за договором № 12 / а і протоколу узгодження ціни № 12 / б.

1. ХАРАКТЕРИСТИКИ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ

- 1.1 Розроблена система методі та засобів захисту даних повинна підтримувати корпоративну мережу типу «зірка» із наступними характеристиками:
- 1.1.1 Повна функціональність 27 робочих станцій.
- 1.1.2 Можливість розширення кількості робочих станцій.
- 1.1.3 Захищеність даних від зовнішніх та внутрішніх загроз.

2. ПРИЗНАЧЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ

- 2.1 Призначення: об'єднання всіх робочих станцій в єдину мережу в єдиному безпековому просторі.
- 2.2 Створення можливості захищеного обміну даних.

3. ОСНОВНІ ВИМОГИ ДО МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ

- 3.1 система методі та засобів захисту даних повинна забезпечувати високу пропускну можливість.
- 3.2 Захищеність і об'єднання в єдиний безпековий простір.
- 3.3 Створення для кожного відділу своїх авторизаційних даних.
- 3.4 Захист від випадкового втручання користувачів до параметрів мережі та сервера.

					ІТС.4КІ.0723.02-ТЗ	Арк.
						3
Змн.	Арк.	№ докум.	Підпис	Дата		

4. ТЕХНІКО-ЕКОНОМІЧНІ ВИМОГИ ДО КІНЦЕВОГО РЕЗУЛЬТАТУ

Вартість розробки данної моделі пристрою визначається згідно з договором на розробку. Вартість розробки повинна бути конкурентноспроможною по відношенню до вже готових пристроїв.

6. ЕТАПИ ВИКОНАННЯ ПР

Етапи виконання ПР можуть уточнювати згідно календарного плану робіт по узгодженню між замовником та виконавцем.

7. ПОРЯДОК ВНЕСЕННЯ ЗМІН ДО ТЕХНІЧНОГО ЗАВДАННЯ, ЩО ЗАТВЕРДЖЕНО

Дане технічне завдання може уточнюватися в процесі розробки ПР при узгодженні сторін з оформленням доповнень до ТЗ.

					ITC.4KI.0723.02-T3	Арк.
						4
Змн.	Арк.	№ докум.	Підпис	Дата		

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЗ «ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА»**

Навчально-науковий інститут фізики, математики та
інформаційних технологій

(назва факультету, інституту)

Інформаційних технологій та систем

(назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

БАКАЛАВРА

(освітньо-кваліфікаційний рівень)

на тему:

**РОЗРОБКА СИСТЕМИ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ В
КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА**

Виконав: студент 4 курсу, групи ____
напряму підготовки (спеціальності)

123 «Комп'ютерна інженерія»

(шифр і назва напряму підготовки, спеціальності)

Берест Р.Ю.

(прізвище та ініціали)

Керівник: **Матієвський В. В.**

(прізвище та ініціали)

Рецензент: **Козуб Ю.Г.**

(прізвище та ініціали)

Миргород – 2023

ЗМІСТ

<u>ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ</u>	7
<u>ВСТУП</u>	9
<u>РОЗДІЛ 1. ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ</u>	11
<u>1.1 Поняття про загрози безпеці інформації</u>	11
<u>1.2 Класифікація загроз безпеки інформації</u>	13
<u>1.3 Найбільш поширені загрози</u>	15
<u>1.3.1 Програмні атаки</u>	17
<u>1.3.2 Шкідливе програмне забезпечення</u>	18
<u>Висновку до розділу 1</u>	19
<u>РОЗДІЛ 2. ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ</u>	21
<u>2.1 Фізичний захист інформації</u>	21
<u>2.2 Апаратні засоби захисту інформації в КМ</u>	24
<u>2.3 Програмні засоби захисту інформації в КМ</u>	26
<u>Висновки до розділу 2</u>	43
<u>РОЗДІЛ 3. МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ</u>	45
<u>3.1 Організаційно-правове забезпечення захисту інформації</u>	45
<u>3.2 Захист інформації в корпоративній мережі на рівні операційної системи</u>	47
<u>3.3 Захист інформації від несанкціонованого доступу</u>	51
<u>3.4 Антивірусний захист</u>	55
<u>Висновки до розділу 3</u>	57
<u>ВИСНОВОК</u>	59
<u>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</u>	62
<u>ДОДАТКИ</u>	64
<u>Додаток А План заходів із захисту інформації в мережі підприємства</u>	64
<u>Додаток Б Основні методи захисту інформації в корпоративній мережі на основі Windows</u>	66

					ІТС.4КІ.0723.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Зміст	Літ.	Арк.	Акрушів	
Розроб.		Берест Р.Ю.							
Керівник		Матієвський В.В.					6	1	
Реценз.		Козуб Ю.Г.				ЛНУ Кафедра ІТС, Гр.4КІ			
Н. Контр.									
Зав. каф.		Семенов М.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СЕБ	Служба економічної безпеки
АІБ	Адміністратор інформаційної безпеки
АІС	Автоматизована інформаційна система
АРМ	Автоматизоване робоче місце
АСУ	Автоматизована система управління
ГТ	Державна таємниця
ДСК	Для службового користування
ЗИ	Захист інформації
ІБ	Інформаційна безпека
ІР	Інформаційний ресурс
ІТ	Інформаційні технології
КТ	Комерційна таємниця
ЛОМ	Локальна обчислювальна мережа
МЕ	Міжмережевий екран
НСД	Несанкціонований доступ
ОІ	Об'єкт інформатизації
ОС	Операційна система
ПЕОМ	Персональна електронна обчислювальна машина
ПЗ	Програмне забезпечення
ПТС	Програмно-технічні засоби
СБП	Служба безпеки підприємства
СВТ	Засоби обчислювальної техніки

					ІТС.4КІ.0723.03-ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата	Перелік умовних позначень		
Розроб.		Берест Р.Ю.					
Керівник		Матієвський В.В.					
Реценз.		Козуб Ю.Г.					
Н. Контр.							
Зав. каф.		Семенов М.А.			ЛНУ Кафедра ІТС, Гр.4КІ.		
					Лім.	Арк.	Акрушів
						7	2

ПЕОМ	Персональна електронна обчислювальна машина
ПЗ	Програмне забезпечення
ПТС	Програмно-технічні засоби
СБП	Служба безпеки підприємства
СВТ	Засоби обчислювальної техніки
СЗІ	Система захисту інформації
ЗКЗІ	Засоби криптозахисту інформації
СОІ	Система обробки інформації
ТСОІ	Технічний засіб обробки інформації
ЕЦП	Електронний цифровий підпис

					ІТС.4КІ.0723.03-ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Проблема захисту інформації є далеко не новою. Вирішувати її люди намагалися в усі віки. На зорі цивілізації цінні відомості зберігалися в матеріальній формі: вирізалися на кам'яних табличках, пізніше записувалися на папір. Для їх захисту використовувалися такі ж матеріальні об'єкти: стіни, рови. Інформація часто передавалася посильними в супроводі охорони. І ці заходи себе виправдовували, оскільки єдиним способом одержання чужої інформації було її викрадення.

Зараз більшість інформації передається в електронному вигляді з допомогою комп'ютерних мереж і спостерігаються такі явища: у сучасному світі злочинці постійно шукають способи зламу та викрадення даних підприємств. Захист інформації стає все складнішим завдяки постійному зростанню кіберзагроз. Багато країн впроваджують законодавчі норми, що обов'язково вимагають від підприємств захищати дані своїх клієнтів. Це ставить підприємства перед викликом розробки ефективних систем захисту даних. Запровадження хмарних обчислень та зберігання даних надає багато переваг, але також створює нові проблеми з безпекою. Підприємства повинні розробляти системи захисту, які забезпечують конфіденційність інформації у хмарних середовищах. Обсяг і цінність даних, що обробляються підприємствами, постійно зростають. Загрози для безпеки даних також стають все більш складними та розповсюдженими. Ефективна система захисту даних є необхідною для запобігання витоку інформації та нанесення шкоди підприємству. Не тільки зовнішні злочинці можуть загрожувати безпеці даних підприємства, але й внутрішні загрози також є серйозним фактором. Працівники, недоброзичливо настроєні співробітники або недосконалі процеси внутрішньої безпеки можуть стати джерелом порушення безпеки даних.

					<i>ІТС.4КІ.0723.03-ПЗ</i>		
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>			
<i>Розроб.</i>		<i>Берест Р.Ю.</i>			<i>Вступ</i>		
<i>Керівник</i>		<i>Матієвський В.В.</i>					
<i>Реценз.</i>		<i>Козуб Ю.Г.</i>					
<i>Н. Контр.</i>							
<i>Зав. каф.</i>		<i>Семенов М.А.</i>					
					<i>Літ.</i>	<i>Арк.</i>	<i>Акрушіє</i>
						9	2
					<i>ЛНУ</i> <i>Кафедра ІТС, Гр.4КІ.</i>		

Система захисту даних повинна враховувати ці аспекти. Усі ці фактори підкреслюють важливість розробки системи методів та засобів захисту даних в комп'ютерній мережі підприємства. Забезпечення безпеки даних є важливим завданням для підприємств у всіх сферах діяльності, і ця тема є актуальною для подальшого розвитку та захисту бізнесу.

Об'єктом дослідження є передача даних в корпоративних мережах.

Предметом дослідження є методи та засоби захисту інформації при передачі даних в корпоративних мережах.

Основною метою роботи є розробка методів та засобів захисту даних в комп'ютерній мережі підприємства.

Для досягнення зазначеної мети необхідно вирішити ряд завдань:

- Розглянути загрози безпеки та їх класифікацію та охарактеризувати найбільш поширені загрози;
- Охарактеризувати методи і засоби захисту інформації в мережі, їх класифікацію та особливості застосування;
- Розкрити можливості фізичних, апаратних та програмних засобів захисту інформації в комп'ютерній мережі (КМ), виявити їх переваги і недоліки;
- Розглянути методи, способи і засоби захисту інформації в корпоративній мережі.

Для вирішення завдань дослідження використано такі **методи дослідження**: *теоретичні*: аналіз наукової літератури, систематизація теоретичних положень про основи захисту інформації; *експериментальні*: тестування розробленої мережі.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1.

ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ

1.1 Поняття про загрози безпеці інформації

Уразливість інформації — це можливість виникнення такого стану, при якому створюються умови для реалізації загроз безпеки інформації.

Атакою на КМ називають дію, застосовану порушником, яке полягає в пошуку й використанні тієї або іншої вразливості. Інакше кажучи, атака на КМ є реалізацією загрози безпеки інформації в ній[1].

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах можна розділити на три основних типи (рис. 1):

перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і надсилається адресату;

підміна авторства інформації. Дана проблема може мати серйозні наслідки. Наприклад, хтось може послати лист від чужого імені або Web-сервер може прикидатися електронним магазином, приймати замовлення, номери кредитних карт, але не висилати ніяких товарів.

					ІТС.4КІ.0723.03-ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Берест Р.Ю.			РОЗДІЛ 1 ОСНОВНІ ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ		Літ.	Арк.
Керівник		Матієвський В.В.						Акрушів
Реценз.		Козуб Ю.Г.					11	11
Н. Контр.							ЛНУ Кафедра ІТС, Гр.4КІ	
Зав. каф.		Семенов М.А..						

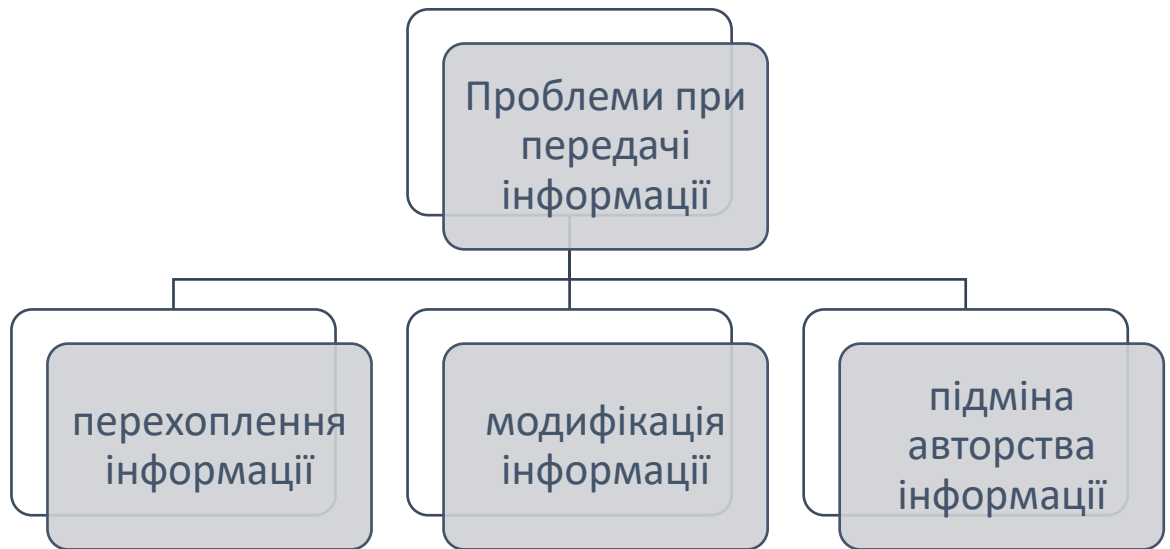


Рис. 1 Основні проблеми, які виникають при передачі інформації

Специфіка комп'ютерних мереж, з точки зору їх уразливості, пов'язана в основному з наявністю інтенсивного інформаційної взаємодії між територіально рознесеними і різнорідними (різнотипними) елементами.

Вразливими є буквально всі основні структурно-функціональні елементи мережі: робочі станції, сервери (Host-машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку і т.п.

Загрози безпеці інформації охоплюють різноманітні ситуації, які можуть призвести до порушення конфіденційності, цілісності та доступності інформації. Вони загрожують безпеці даних, інформаційних систем, мереж та комунікаційних каналів. Основні поняття, пов'язані з загрозами безпеці інформації, включають[5, 7]:

Кібератаки: Це зловмисні дії, спрямовані на злам інформаційних систем і мереж з метою незаконного доступу до даних, крадіжки інформації, внесення змін у системи або завдання шкоди.

Віруси і шкідливі програми: Це програми, які розповсюджуються інфекційним шляхом та можуть пошкодити системи, викрадати дані або виконувати зловмисні дії без дозволу користувача.

Фішинг: Це вид атаки, при якій зловмисники намагаються отримати конфіденційну інформацію, таку як паролі, номери кредитних карток або особисті дані, шляхом імітації довіреної сторони, часто через підроблені електронні листи або веб-сайти.

Деніал сервісу (DoS) і розподілений деніал сервісу (DDoS): Це атаки, спрямовані на перевантаження цільової системи або мережі, заважаючи їм нормально функціонувати та доступу до них користувачів.

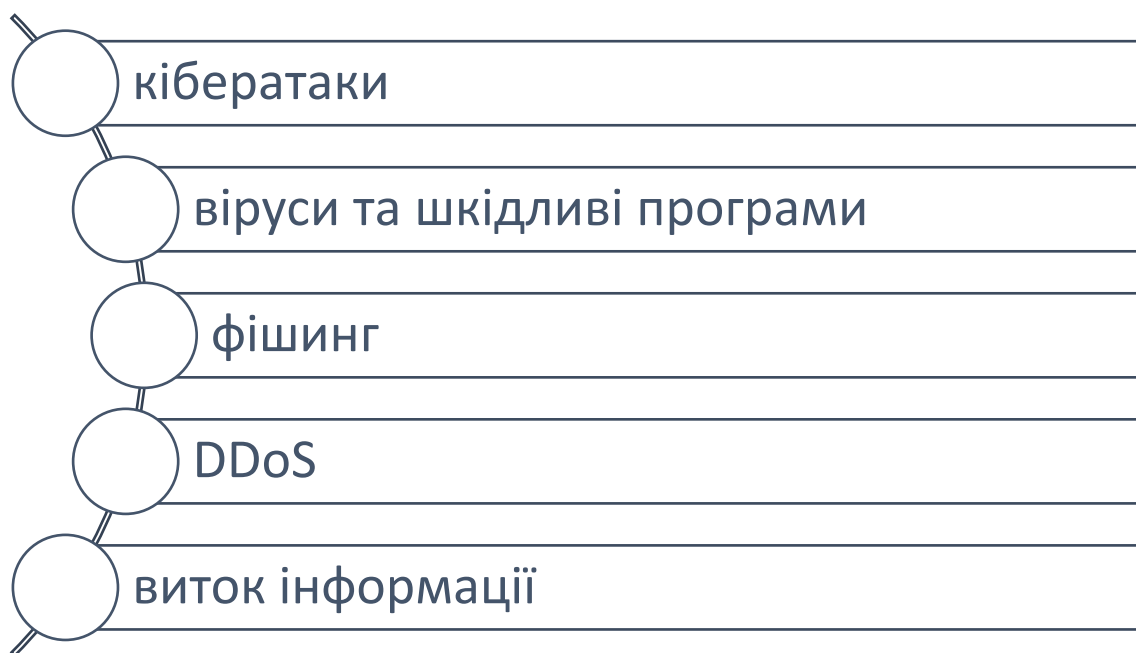


Рис. 2 Основи загрози безпеці інформації

1.2 Класифікація загроз безпеки інформації

Відома велика кількість різнопланових загроз безпеки інформації різного походження. У літературі зустрічається безліч різноманітних класифікацій, де в якості критеріїв поділу використовуються види породжуваних небезпек, ступінь злого умислу, джерела появи загроз і т.п.

- Природні загрози - це загрози, викликані впливами на КМ та її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

- Штучні загрози - це загрози КМ, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:
 - ненавмисні (випадкові) загрози, викликані помилками в проектуванні КМ та її елементів, помилками в програмному забезпеченні, помилками в діях персоналу тощо;
 - навмисні загрози, пов'язані з корисливими намірами людей (зловмисників).

Джерела загроз по відношенню до КМ можуть бути зовнішніми або внутрішніми (компоненти самої КМ - її апаратура, програми, персонал).

Аналіз негативних наслідків реалізації загроз передбачає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, які сприяють їх прояву і методів реалізації.

Загрози класифікуються по можливості заподіяння шкоди суб'єкту при порушенні порядку безпеки. Збиток може бути заподіяний яким-небудь суб'єктом (злочин, вина або недбалість), а також стати наслідком, що не залежать від суб'єкт. Загроз не так вже й багато. При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації та засобів її обробки, а також її втрата (ненавмисна). При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення достовірності інформації; нав'язування неправдивої інформації. При забезпеченні доступності інформації можливе її блокування або знищення самої інформації та засобів її обробки.

Всі джерела загроз можна розділити на класи, обумовлені типом носія, а класи на групи по місцю розташування. Проблеми також можна розділити на класи по відносності до джерела, а класи на групи і підгрупи по місцезнаходженню. Методи реалізації можна поділити на групи за можливою реалізацією. При цьому необхідно враховувати, що саме поняття «метод», застосовується лише при розгляді реалізації загроз антропогенними

					ІТС.4КІ.0723.03-ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

джерелами. Для техногенних та стихійних джерел це поняття трансформується в поняття «передумова».

Класифікація можливостей реалізації загроз (атак), являє собою сукупність можливих варіантів дій джерела загроз певними методами реалізації з використанням вразливостей, які приводять до реалізації цілей атаки. Мета атаки може не збігатися з метою реалізації загроз і може бути спрямована на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози. У разі такого неспівпадіння атака розглядається як етап підготовки до вчинення ряду дій, спрямованих на реалізацію загрози, тобто як «підготовка до вчинення» протиправної дії. Результатом атаки є наслідки, які є реалізацією загрози і/або сприяють такій реалізації.

Вихідними даними для проведення оцінки і аналізу загроз безпеки при роботі в мережі служать результати анкетування суб'єктів відносин, спрямовані на з'ясування спрямованості їх діяльності, передбачуваних пріоритетів цілей безпеки, завдань, розв'язуваних в мережі і умов розташування та експлуатації мережі.

1.3 Найбільш поширені загрози

Найбільш частими і найбільш небезпечними (з точки зору розміру збитку) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують комп'ютерну мережу.

Іноді такі помилки і є власне загрозами (неправильно введені дані або помилки в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (зазвичай це помилки адміністрування). За деякими даними, до 72% втрат - наслідок ненавмисних помилок.

Пожежі і повені не приносять стільки лиха, скільки безграмотність і недбалість працівників.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

Очевидно, найрадикальнiй спосiб боротьби з ненавмисними помилками - максимальна автоматизацiя i суворий контроль.

Иншi загрози доступностi можна класифiкувати за компонентами КМ, на якi нацiленi загрози[13]:

- вiдмова користувачiв;
- внутрiшня вiдмова мережi;
- вiдмова пiдтримуючої iнфраструктури.

Зазвичай стосовно користувача розглядаються такi загрози:

- небажання працювати з iнформацiйною системою (найчастiше проявляється при необхідностi освоювати новi можливостi та при розходженнi мiж запитами користувачiв i фактичними можливостями та технiчними характеристиками);
- неможливість працювати з системою в силу вiдсутностi вiдповiдної пiдготовки (недолiк загальної комп'ютерної грамотностi, невмiння iнтерпретувати дiагностичнi повiдомлення, невмiння працювати з документацiєю тощо);
- неможливість працювати з системою в силу вiдсутностi технiчної пiдтримки (неповнота документацiї, недолiк довідкової iнформацiї тощо).

Основними джерелами внутрiшнiх вiдмов є:

вiдступ (випадкове або навмисне) вiд встановлених правил експлуатацiї;

- вихiд системи iз штатного режиму експлуатацiї в силу випадкових або навмисних дiй користувачiв або обслуговуючого персоналу (перевищення розрахункового числа запитiв, надмiрний обсяг оброблюваної iнформацiї тощо);
- помилки при конфiгуруваннi та переконфiгуруваннi системи;
- вiдмови програмного i апаратного забезпечення;
- пошкодження даних;
- пошкодження апаратури.

По відношенню до підтримуючої інфраструктури рекомендується розглядати такі загрози:

- порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо - та/або повітряпостачання, кондиціонування;
- пошкодження приміщень;
- неможливість або небажання обслуговуючого персоналу або користувачів виконувати свої обов'язки (цивільні порушення, аварії на транспорті, терористичний акт або його загроза, страйк тощо).
- "ображені" співробітники - нинішні і колишні. Як правило, вони прагнуть нанести шкоду організації - "кривднику", наприклад:
 - зіпсувати обладнання;
 - вбудувати логічну бомбу, яка з часом зруйнує програми або дані;
 - видалити дані.

Скривджені співробітники, навіть колишні, знайомі з порядками в організації і здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні працівника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

1.3.1 Програмні атаки

В якості засобу виведення мережі з штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – пропускну можливості мережі, обчислювальних можливостей процесорів або оперативної пам'яті). За розташуванням джерела загрози таке споживання поділяється на локальне та віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор і/або фізичну пам'ять, звівши швидкість виконання інших програм до нуля[8].

Найпростіший приклад віддаленого споживання ресурсів - атака, яка отримала найменування "SYN-повінь". Вона являє собою спробу заповнити таблицю "напіввідкритих" TCP-з'єднань сервера (встановлення з'єднань

					ІТС.4КІ.0723.03-ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

починається, але не закінчується). Така атака найменшою мірою ускладнює встановлення нових з'єднань зі сторони авторизованих користувачів, тобто сервер виглядає як недоступний.

По відношенню до атаки "Papa Smurf" вразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети "з'їдають" пропускну спроможність мережі.

Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі - як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком звичайні запити на з'єднання та обслуговування. Часом початку "моди" на подібні атаки можна вважати лютий 2000 року, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше - власники та користувачі систем). Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускнуою спроможністю мережі та продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко.

Для виведення систем із штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних та апаратних помилок. Наприклад, відома помилка в процесорі Pentium I давала можливість локальному користувачеві шляхом виконання певної команди "підвісити" комп'ютер, так що допомагає тільки апаратний RESET.

Програма "Teardrop" віддалено "підвішує" комп'ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів.

1.3.2 Шкідливе програмне забезпечення

Одним з найнебезпечніших способів проведення атак є впровадження в атаковані системи шкідливого програмного забезпечення[2].

Виділяють наступні аспекти шкідливого ПЗ:

- шкідлива функція;
- спосіб поширення;
- зовнішнє подання.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

Частина, що здійснює руйнівну функцію, призначається для:

- впровадження іншого шкідливого ПЗ;
- отримання контролю над атакуємою системою;
- агресивного споживання ресурсів;
- зміни або руйнування програм та даних.

За механізмом поширення розрізняють:

- віруси - код, що володіє здатністю до поширення (можливо, зі змінами) шляхом впровадження в інші програми;
- черв'яки - код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по мережі і їх виконання (для активізації вірусу потрібно запуск зараженої програми).

Віруси зазвичай поширюються локально, в межах вузла мережі; для передачі по мережі їм потрібна зовнішня допомога, така як пересилання зараженого файлу. "Черв'яки", навпаки, орієнтовані в першу чергу на подорожі по мережі.

Іноді саме поширення шкідливого ПЗ викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, "черв'яки", "з'їдають" смугу пропускання мережі і ресурси поштових систем.

Шкідливий код, який виглядає як функціонально корисна програма, називається троянським. Наприклад, звичайна програма, будучи зараженою вірусом, стає троянською; деколи троянські програми виготовляють вручну та підсовують довірливим користувачам в будь-якій привабливій обгортці (зазвичай при відвідуванні файлообмінних мереж або ігрових і розважальних сайтів).

Висновку до розділу 1

Досліджено поняття «загроза безпеці інформації» та визначено, що це потенційна небезпека або вразливість, яка може призвести до незаконного доступу, руйнування, втрати, розкриття або порушення цілісності інформації

					ІТС.4КІ.0723.03-ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

Вона може включати дії або події, спрямовані на компрометацію безпеки даних, систем або мереж.

Загрози безпеці інформації можуть походити як зовнішньо (зловмисні хакери, кіберзлочинці, краудсорсинг атаки), так і зсередини організації (інсайдери, недбалість персоналу). Вони можуть включати такі види атак, як вторгнення в мережу, віруси, фішинг, спуфінг, деніал-сервіс атаки, крадіжку даних, шкідливі програми і багато інших.

Загрози безпеці інформації можуть мати серйозні наслідки для організації, включаючи втрату конфіденційності даних, порушення цілісності інформації, втрату доступу до важливих ресурсів, фінансові втрати, псування репутації організації та вплив на її бізнес-операції.

Наведено класифікації загроз безпеки інформації та охарактеризовано найбільш поширені загрози.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2.

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ

Розібрати детально всі методи і засоби захисту інформації в рамках роботи досить складно, але ми зможемо схарактеризувати тільки деякі з них.

2.1 Фізичний захист інформації

До заходів фізичного захисту інформації відносяться:

- захист від вогню;
- захист від води і пожежогасячої рідини
- захист від корозійних газів;
- захист від електромагнітного випромінювання;
- захист від вандалізму;
- захист від крадіжки і крадіжки;
- захист від вибуху;
- захист від падаючих уламків;
- захист від пилу;
- захист від несанкціонованого доступу в приміщення.

Які ж дії потрібно зробити, щоб забезпечити фізичну безпеку?

В першу чергу треба підготувати приміщення, де будуть стояти host-машини. Обов'язкове правило: сервер повинен знаходитися в окремій кімнаті, доступ до якої повинен бути обмежений невеликим колом осіб. У цьому приміщенні слід встановити кондиціонер і хорошу систему вентиляції. Також можливо помістити системи безперебійного електроживлення.

					ІТС.4КІ.0723.03-ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Берест Р.Ю.			РОЗДІЛ 2 ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ		Літ.	Арк.
Керівник		Матієвський В.В.						
Реценз.		Козуб Ю.Г.						
Н. Контр.								
Зав. каф.		Семенов М.А..						
							21	2
						ЛНУ Кафедра ІТС, Гр.4КІ		

Розумним кроком стане відключення невикористовуваних паралельних і послідовних портів сервера. Його корпус бажано опечатати. Все це ускладнить крадіжку або підміну інформації навіть у тому випадку, якщо зловмисник якимось чином проникне в серверну кімнату. Не варто нехтувати і такими тривіальними заходами захисту, як залізні ґрати і двері, кодові замки і камери відеоспостереження, які будуть постійно вести запис усього, що відбувається в ключових приміщеннях офісу[7].

Інша характерна помилка пов'язана з резервним копіюванням. Про його необхідність знають всі, так само як і про те, що на випадок пожежі треба мати вогнегасник. А от про те, що резервні копії можна зберігати в різних приміщеннях з сервером, чомусь забувають. В результаті, захистившись від інформаційних атак, фірми виявляються беззахисними навіть перед невеликим пожежею, в якому завбачливо зроблені копії гинуть разом з сервером.

Часто, навіть захистивши сервери, забувають, що захисту потребують і всіляка кабельна система мережі. Причому, нерідко доводиться побоюватися не зловмисників, а самих звичайних прибиральниць, які заслужено вважаються найстрашнішими ворогами локальних мереж. Найкращий варіант захисту кабелю - це короби, але, в принципі, підійде будь-який інший спосіб, що дозволяє приховати і надійно закріпити дроти. Втім, не варто випускати з виду і можливість підключення до них ззовні для перехоплення інформації або створення перешкод, наприклад, за допомогою розряду струму. Хоча, треба визнати, що цей варіант мало поширений і помічений лише при порушеннях роботи великих фірм.

Крім Інтернету, комп'ютери включені ще одну мережу - звичайну електричну. Саме з нею пов'язана інша група проблем, що відносяться до фізичної безпеки серверів. Ні для кого не секрет, що якість сучасних силових мереж далека від ідеалу. Навіть якщо немає ніяких зовнішніх ознак аномалій, дуже часто напруга в електромережі вище або нижче норми. При цьому

					ІТС.4КІ.0723.03-ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

більшість людей навіть не підозрюють, що в їх будинку або офісі існують якісь проблеми з електроживленням.

Знижена напруга є найбільш поширеною аномалією і складає близько 85% від загального числа різних неполадок з електроживленням. Його звичайна причина - дефіцит електроенергії, який особливо характерний для зимових місяців. Підвищена напруга майже завжди є наслідком якої-небудь аварії або пошкодження проводки в приміщенні. Часто в результаті від'єднання загального нульового проводу сусідні фази виявляються під напругою 380 Вт. Буває також, що висока напруга виникає в мережі із-за неправильної комутації проводів.

Джерелами імпульсних і високочастотних перешкод можуть стати розряди блискавок, включення або відключення потужних споживачів електроенергії, аварії на підстанціях, а також робота деяких побутових електроприладів. Найчастіше такі перешкоди виникають у великих містах і промислових зонах. Імпульси напруги при тривалості від наносекунд до мікросекунд можуть по амплітуді досягати декількох тисяч вольт. Найбільш вразливими до таких перешкод виявляються мікропроцесори та інші електронні компоненти. Нерідко непогашена імпульсна перешкода може призвести до перезавантаження сервера або помилку в обробці даних. Вбудований блок живлення комп'ютера, звичайно, частково згладжує імпульси напруги, захищаючи електронні компоненти комп'ютера від виходу з ладу, але залишкові перешкоди все одно знижують термін служби апаратури, а також призводять до зростання температури в блоці живлення сервера.

Для захисту комп'ютерів від високочастотних імпульсних завад служать мережеві фільтри, що оберігають техніку від більшості перешкод і перепадів напруги. Крім того, комп'ютери з важливою інформацією слід обов'язково оснащувати джерелом безперебійного живлення (UPS). Сучасні моделі UPS не тільки підтримують роботу комп'ютера, коли пропадає

					ІТС.4КІ.0723.03-ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

живлення, але і від'єднують його від електромережі, якщо параметри електромережі виходять з допустимого діапазону.

2.2 Апаратні засоби захисту інформації в КМ

До апаратних засобів захисту інформації відносяться електронні та електронно-механічні пристрої, що включаються до складу технічних засобів КМ і виконують (самостійно або в єдиному комплексі з програмними засобами) деякі функції забезпечення інформаційної безпеки. Критерієм віднесення пристрою до апаратних, а не до інженерно-технічних засобів захисту є обов'язкове включення до складу технічних засобів КМ[9].

До основних апаратних засобів захисту інформації відносяться:

- пристрої для введення ідентифікує користувача інформації (магнітних і пластикових карт, відбитків пальців тощо);
- пристрої для шифрування інформації;
- пристрої для перешкоджання несанкціонованому включенню робочих станцій і серверів (електронні замки і блокатори).

Приклади допоміжних апаратних засобів захисту інформації:

- пристрої знищення інформації на носіях;
- пристрої сигналізації при спробах несанкціонованих дій користувачів КМ.

Апаратні засоби привертають все більшу увагу фахівців не тільки тому, що їх легше захистити від пошкоджень і інших випадкових або злочинних дій, але ще й тому, що апаратна реалізація функцій вище за швидкодією, ніж програмна, а вартість їх неухильно знижується.

Апаратні засоби захисту інформації включають фізичні пристрої, компоненти та системи, які використовуються для забезпечення безпеки даних і захисту від різних загроз. Ці засоби можуть забезпечувати захист на різних рівнях, від захисту окремих пристроїв до захисту всієї інфраструктури мережі. Ось кілька основних видів апаратних засобів захисту інформації:

					ІТС.4КІ.0723.03-ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Брандмауери (Firewalls): Брандмауери - це пристрої, які контролюють трафік мережі та фільтрують небажаний або шкідливий трафік. Вони дозволяють встановлювати правила і політики безпеки, що обмежують доступ до ресурсів мережі і захищають їх від несанкціонованого доступу.

2. Інтрузійні виявлення і запобігання (Intrusion Detection and Prevention Systems, IDS/IPS): Ці системи моніторять мережевий трафік з метою виявлення незвичайної або підозрілої активності, яка може бути пов'язана зі зловмисними атаками. IDS/IPS можуть виявляти вторгнення та приймати заходи для їх запобігання або реагування на них.

3. Криптографічні модулі та пристрої: Криптографічні модулі та пристрої використовуються для шифрування та розшифрування даних з метою забезпечення конфіденційності інформації. Вони використовують різні алгоритми шифрування, такі як AES (Advanced Encryption Standard) або RSA (Rivest-Shamir-Adleman), для захисту даних від несанкціонованого доступу.

4. Фізичні бар'єри та контроль доступу: Ці засоби включають системи контролю доступу, які забезпечують фізичний захист об'єктів і обмежують доступ до них. Це можуть бути картки доступу, біометричні системи (відбитки пальців, сканування обличчя) або фізичні бар'єри, такі як замки і пропускні пункти.

5. Захист від перенапруг: Ці пристрої призначені для захисту електронної техніки від несприятливих електричних перепадів, таких як перенапруги або блискавки. Вони забезпечують стабільну живлення і захист від можливих пошкоджень, що можуть виникнути внаслідок електричних неполадок.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 3 Апаратні засоби захисту інформації

Ці апаратні засоби захисту інформації працюють у поєднанні з програмним забезпеченням та процедурами безпеки, щоб створити комплексний підхід до захисту даних і забезпечити високий рівень безпеки для підприємства. Вибір конкретних апаратних засобів захисту залежить від потреб і вимог підприємства, а також від типу даних та ризиків, з якими воно стикається.

2.3 Програмні засоби захисту інформації в КМ

Під програмними засобами захисту інформації розуміють спеціальні програми, які включаються до складу програмного забезпечення КМ виключно для виконання захисних функцій.

До основних програмних засобів захисту інформації відносяться[11]:

- програми ідентифікації і аутентифікації користувачів КМ;
- програми розмежування доступу користувачів до ресурсів КМ;
- програми шифрування інформації;
- програми захисту інформаційних ресурсів (системного та

прикладного програмного забезпечення, баз даних, комп'ютерних

засобів навчання і т. п.) від несанкціонованої зміни, використання та копіювання.

Треба розуміти, що під ідентифікацією, стосовно забезпечення інформаційної безпеки КМ, розуміють однозначне розпізнавання унікального імені суб'єкта КМ. Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає даному суб'єкту (підтвердження достовірності суб'єкта).

Також до програмних засобам захисту інформації відносяться:

- програми знищення залишкової інформації (в блоках оперативної пам'яті, тимчасових файлах тощо);
- програми аудиту (ведення реєстраційних журналів) подій, пов'язаних з безпекою КМ, для забезпечення можливості відновлення і докази факту події цих подій;
- програми імітації роботи з порушником (відволікання його на нібито отримання конфіденційної інформації);
- програми тестового контролю захищеності КМ тощо.

До переваг програмних засобів захисту інформації відносяться:

- простота тиражування;
- гнучкість (можливість налаштування на різні умови застосування, що враховують специфіку загроз інформаційної безпеки конкретних КМ);
- простота застосування — одні програмні засоби, наприклад шифрування, працюють у «прозорому» (непомітному для користувача) режимі, а інші не потребують від користувача ніяких нових (порівняно з іншими програмами) навичок;
- практично необмежені можливості їх розвитку шляхом внесення змін для обліку нових загроз безпеки інформації.

До недоліків програмних засобів захисту інформації відносяться:

- зниження ефективності КМ за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;

					ІТС.4КІ.0723.03-ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

- більш низька продуктивність (порівняно з аналогічним функціоналом апаратними засобами захисту, наприклад шифрування);
- залежність багатьох програмних засобів захисту, що створює для порушника принципову можливість їх обходу;
- можливість зловмисного зміни програмних засобів захисту в процесі експлуатації КМ.

Безпека на рівні операційної системи

Операційна система є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки у кожній конкретній ОС багато в чому залежить і загальна безпека інформаційної системи.

Операційна система MS-DOS є ОС реального режиму мікропроцесора Intel, а тому тут не може йти мови про розподіл оперативної пам'яті між процесами. Всі резидентні програми і основна програма використовують загальний простір ОЗП. Захисту файлів немає, про мережевої безпеки важко сказати щось певне, бо на тому етапі розвитку драйвери для мережевої взаємодії розроблялися не фірмою Microsoft, а сторонніми розробниками.

Сімейство операційних систем Windows 95, 98, Millenium – це клони, орієнтовані на роботу в домашніх ЕОМ. Ці операційні системи використовують рівні привілеїв захищеного режиму, але не роблять ніяких додаткових перевірок не підтримують системи дескрипторів безпеки. У результаті цього будь-який додаток може отримати доступ до всього обсягу доступної оперативної пам'яті як з правами читання, так і з правами запису. Заходи мережевої безпеки присутні, проте їх реалізація не на висоті. Більш того, в версії Windows 95 була допущена ґрунтовна помилка, яка дозволяє віддалено буквально за кілька пакетів приводити до "зависання" ЕОМ, що значно підірвало репутацію ОС, у наступних версіях було зроблено багато кроків по поліпшенню мережевої безпеки цього клону.

Покоління операційних систем Windows NT, 2000 вже значно більше надійний розробка компанії Microsoft. Вони є дійсно розрахованими на

					ІТС.4КІ.0723.03-ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

великі системи, які надійно захищають файли різних користувачів на жорсткому диску (правда, шифрування даних все ж не виробляється і файли можна без проблем прочитати, завантажившись з диска іншої операційної системи – наприклад, MS-DOS). Дані ОС активно використовують можливості захищеного режиму процесорів Intel, і можуть надійно захистити дані та код процесу від інших програм, якщо тільки він сам не захоче надавати до них додаткового доступу ззовні процесу.

За довгий час розробки було враховано безліч різних мережесих атак і помилок в системі безпеки. виправлення до них виходили у вигляді блоків оновлень (service pack).

Інша гілка клонів зростає від операційної системи UNIX. Ця ОС спочатку розроблялася як мережна, а тому одразу ж містила в собі засоби інформаційної безпеки. Практично все широко розповсюджені клон UNIX пройшли довгий шлях розробки і по мірі модифікації врахували всі відкриті за цей час способи атак. Досить добре себе зарекомендували: LINUX (S.U.S.E.), OpenBSD, FreeBSD, Sun Solaris. Отже все сказане відноситься до останніх версій цих операційних систем. Основні помилки в цих системах відносяться вже не до ядра, яке працює бездоганно, а до системним і прикладним утилітам. наявність помилок в них часто приводить до втрати всього запасу міцності системи.

Основні компоненти[13]:

LSA – несе відповідальність за несанкціонований доступ, перевіряє повноваження користувача на вхід в систему, підтримує:

- Аудит – перевірка правильності виконання дій користувача
- Диспетчер облікових записів – підтримка БД користувачів їх дій та взаємодії з системою.
- Монітор безпеки – перевіряє чи користувач має достатні права доступу на об'єкт;
- Журнал аудиту – містить інформацію про входи користувачів, фіксує роботи з файлами, папками.

- Пакет аутентифікації – аналізує системні файли на предмет того, що вони не замінені. MSV10 – пакет за замовчуванням.

В Windows – більш повне і глибоке диференціювання прав доступу користувача.

EFS – забезпечує шифрування і дешифрування інформації (файли і папки) для обмеження доступу до даних.

Криптографічні методи захисту

Криптографія - це наука про забезпечення безпеки даних. Вона займається пошуками рішень чотирьох важливих проблем безпеки, конфіденційності, аутентифікації, цілісності і контролю учасників взаємодії. Шифрування - це перетворення даних в нечитабельну форму, використовуючи ключі шифрування-розшифровки. Шифрування дозволяє забезпечити конфіденційність, зберігаючи інформацію в таємниці від того, кому вона не призначена.

Криптографія займається пошуком і дослідженням математичних методів перетворення інформації.

Сучасна криптографія містить у собі чотири великих розділи[10]:

- симетричні криптосистеми;
- криптосистеми з відкритим ключем;
- системи електронного підпису;
- управління ключами.

Основні напрямки використання криптографічних методів - передача конфіденційної інформації через канали зв'язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді.

Шифрування дисків

Зашифрований диск – це файл-контейнер, усередині якого можуть знаходитися будь-які інші файли або програми (вони можуть бути встановлені і запущені прямо з цього зашифрованого файлу). Цей диск доступний тільки після введення пароля до файлу-контейнера – тоді на

					<i>ІТС.4КІ.0723.03-ПЗ</i>	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

комп'ютері з'являється ще один диск, ця особа системою як логічний і робота з яким не відрізняється від роботи з будь-яким іншим диском. Після відключення диска логічний диск зникає, він стає «невидимим».

На сьогоднішній день найбільш поширені програми для створення зашифрованих дисків – DriveCrypt, BestCrypt і PGPdisk. Кожна з них надійно захищена від віддаленого злому.

Загальні риси програм:

- всі зміни інформації у файлі-контейнері відбуваються спочатку в оперативній пам'яті, тобто жорсткий диск завжди залишається зашифрованим. Навіть у випадку зависання комп'ютера секретні дані залишаються зашифрованими;
- програми можуть блокувати прихований логічний диск після закінчення певного проміжку часу;
- всі вони недовіжливо ставляться до тимчасових файлів (свап-файлів). Є можливість шифрувати всю конфіденційну інформацію, яка могла потрапити в свап-файл. Дуже ефективний метод приховування інформації, що зберігається в свап-файл – це взагалі вимкнути його, при цьому не забувши наростити оперативну пам'ять комп'ютера;
- фізика жорсткого диска така, що навіть якщо поверх одних даних записати інші, то попередній запис повністю не зітреться. З допомогою сучасних засобів магнітної мікроскопії (Magnetic Force Microscopy – MFM) їх все одно можна відновити. За допомогою цих програм можна надійно видаляти файли з жорсткого диска, не залишаючи ніяких слідів їх існування;
- всі три програми зберігають конфіденційні дані надійно шифруються на жорсткому диску і забезпечують прозорий доступ до цих даних з будь-якої прикладної програми;
- вони захищають зашифровані файли-контейнери від випадкового видалення;
- відмінно справляються з троянськими програмами та вірусами.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

Способи ідентифікації користувача

Перш ніж отримати доступ до ВС, користувач повинен ідентифікувати себе, а механізми захисту мережі потім підтверджують справжність користувача, тобто перевіряють, чи користувач є дійсно тим, за кого він себе видає. У відповідності з логічною моделлю механізму захисту ЗС розміщені на робочій ЕОМ, до якої підключений користувач через свій термінал або яким-небудь іншим способом. Тому процедури ідентифікації, автентифікації та наділення повноваженнями виконуються до початку сеансу на місцевій робочій ЕОМ.

Надалі, коли встановлюються різні мережеві протоколи і до отримання доступу до мережевих ресурсів, процедури ідентифікації, автентифікації та наділення повноваженнями можуть бути активізовані знову на деяких віддалених робочих ЕОМ з метою розміщення необхідних ресурсів або мережевих послуг.

Коли користувач починає роботу в обчислювальній системі, використовуючи термінал, система запитує його ім'я та ідентифікаційний номер. Згідно з відповідями користувача обчислювальна система виробляє його ідентифікацію. У мережі більш природно для об'єктів, що встановлюють взаємну зв'язок, ідентифікувати один одного.

Паролі - це лише один із способів підтвердження автентичності. Існують інші способи:

- Зумовлена інформація, яка знаходиться у розпорядженні користувача: пароль, особистий ідентифікаційний номер, угода про використання спеціальних закодованих фраз.
- Елементи апаратного забезпечення, що знаходяться в розпорядженні користувача: ключі, магнітні картки, мікросхеми і т. п..
- Характерні особисті особливості користувача: відбитки пальців, малюнок сітківки ока, розміри фігури, тембр голосу і інші більш складні медичні та біохімічні властивості.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

- Характерні прийоми і риси поведінки користувача в режимі реального часу: особливості динаміки, стиль роботи на клавіатурі, швидкість читання, вміння використовувати маніпулятори і т. д.
- Звички: використання специфічних комп'ютерних заготовок.
- Навички та знання користувача, обумовлені освітою, культурою, навчанням, передісторією, вихованням, звичками тощо.

Якщо хтось бажає увійти в обчислювальну систему через термінал або виконати пакетне завдання, обчислювальна система повинна встановити справжність користувача. Сам користувач, як правило, не перевіряє справжність обчислювальної системи. Якщо процедура встановлення автентичності є односторонньою, таку процедуру називають процедурою одностороннього підтвердження автентичності об'єкта[13] .

Спеціалізовані програмні засоби захисту інформації

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби мережесих ОС. Крім програм шифрування, існує багато інших доступних зовнішніх засобів захисту інформації. З найбільш часто згадуваних слід відзначити наступні дві системи, що дозволяють обмежити інформаційні потоки.

Firewalls - брандмауери (дослівно firewall — вогняна стіна). Між локальною і глобальною мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь що проходить через них трафік мережевого/ транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку зовсім. Більш захищена різновид методу - це спосіб маскування (masquerading), коли весь вихідний з локальної мережі трафік надсилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

Проку-сервери (проку - довіреність, довірена особа). Весь трафік мережевого/транспортного рівнів між локальною і глобальною мережами забороняється повністю — просто відсутня маршрутизація як така, а

					ІТС.4КІ.0723.03-ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому методі звернення з глобальної мережі в локальну стають неможливими в принципі. Очевидно також, що цей метод не дає достатнього захисту проти атак на більш високих рівнях - наприклад, на рівні програми (віруси, код Java і JavaScript).

Розглянемо детальніше роботу брандмауера. Це метод захисту мережі від загроз, що виходять від інших систем та мереж, з допомогою централізації доступу до мережі і контролю за ним апаратно-програмними засобами. Брандмауер є захисним бар'єром, що складається з декількох компонентів (наприклад, маршрутизатора або шлюзу, на якому працює програмне забезпечення брандмауера). Брандмауер конфігурується у відповідності з прийнятою політикою організації контролю доступу до внутрішньої мережі. Всі вхідні і вихідні пакети повинні проходити через брандмауер, який пропускає тільки авторизовані пакети.

Брандмауер з фільтрацією пакетів [packet-filtering firewall] - є маршрутизатором або комп'ютером, на якому працює програмне забезпечення, налаштоване таким чином, щоб відбракувати певні види вхідних і вихідних пакетів. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP і IP - заголовках пакетів (адреси відправника та одержувача, їх номери портів тощо).

Брандмауер експертного рівня [stateful inspection firewall] - перевіряє вміст прийнятих пакетів на трьох рівнях моделі OSI - мережна, сеансовому і прикладному. Для виконання цього завдання використовуються спеціальні алгоритми фільтрації пакетів, за допомогою яких кожен пакет порівнюється з відомим шаблоном авторизованих пакетів.[9]

Створення брандмауера відноситься до вирішення завдання екранування. Формальна постановка завдання захисту полягає в наступному. Нехай є дві безлічі інформаційних систем. Екран - це засіб розмежування доступу клієнтів з однієї безлічі серверів з іншого безлічі. Екран виконує свої функції, контролюючи всі інформаційні потоки

					ІТС.4КІ.0723.03-ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

між цими двома безлічами систем (рис. 6). Контроль потоків складається в їхній фільтрації, можливо, з виконанням деяких перетворень.

На наступному рівні деталізації екран (напівпроникну мембрану) зручно представляти як послідовність фільтрів. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу "перекинути" через екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу чи опрацювання даних від імені адресата і повернення результату відправнику.

Крім функцій, розмежування доступу, екрани здійснюють протоколювання обміну інформацією.

Зазвичай екран не є симетричним, для нього визначено поняття "усередині" і "зовні". При цьому завдання екранування формуються як захист внутрішньої області від потенційно ворожої зовнішньої. Так, міжмережеві екрани (ME) найчастіше встановлюють для захисту корпоративної мережі організації, що має вихід в Internet.

Екранування допомагає підтримувати доступність сервісів внутрішньої області, зменшуючи або взагалі ліквідуючи навантаження, викликане зовнішньою активністю. Зменшується вразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен подолати екран, де захисні механізми сконфігуровані особливо ретельно. Крім того, екранує система, на відміну від універсальної, може бути влаштована більш простим і, отже, більш безпечним чином.

Екранування дає можливість контролювати також інформаційні потоки, спрямовані в зовнішню область, що сприяє підтримці режиму конфіденційності в організації.

Екранування може бути частковим, захищає певні інформаційні сервіси (наприклад, екранування електронної пошти).

Обмежуючий інтерфейс також можна розглядати як різновид екранування. На невидимий об'єкт важко нападати, особливо за допомогою фіксованого набору засобів. У цьому змісті Web-інтерфейс має природним

					ІТС.4КІ.0723.03-ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

захистом, особливо в тому випадку, коли гіпертекстові документи формуються динамічно. Кожен користувач бачить лише те, що йому належить бачити. Можна провести аналогію між динамічно формуються гіпертекстовими документами і поданнями в реляційних базах даних, з тією суттєвою застереженням, що в разі Web можливості істотно ширше.

Екрануюча роль Web-сервісу наочно виявляється і тоді, коли цей сервіс здійснює посередницькі (точніше, що інтегрують) функції при доступі до інших ресурсів, зокрема таблицям бази даних. Тут не тільки контролюються потоки запитів, але і ховається реальна організація даних.

Архітектурні аспекти безпеки

Боротися з погрозами, властивому мережному середовищі, засобами універсальних операційних систем не представляється можливим. Універсальна ОС - це величезна програма, що напевно містить, крім явних помилок, деякі особливості, які можуть бути використані для нелегального отримання привілеїв. Сучасна технологія програмування не дозволяє зробити настільки великі програми безпечними. Крім того, адміністратор, що має справу зі складною системою, далеко не завжди в стані врахувати всі наслідки вироблених змін. Нарешті, в універсальній багатокористувацької системі пролому в безпеці постійно створюються самими користувачами (слабкі чи, рідко змінювані паролі, невдало встановлені права доступу, залишений без догляду термінал і т. п.). Єдиний перспективний шлях зв'язаний з розробкою спеціалізованих сервісів безпеки, які в силу своєї простоти допускають формальну чи неформальну верифікацію. Міжмережевий екран саме і є таким засобом, що допускає подальшу декомпозицію, зв'язану з обслуговуванням різних мережних протоколів.

Міжмережевий екран розташовується між що захищається (внутрішньої) мережею і зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішнє МЕ, у другому - про внутрішній. Залежно від точки зору, зовнішній

					ІТС.4КІ.0723.03-ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

міжмережевий екран можна вважати першою або останньою (але не єдиною) лінією оборони. Першою - якщо дивитися на світ очима зовнішнього злоумисника. Останній - якщо прагнути до захищеності всіх компонентів корпоративної мережі та припинення неправомірних дій внутрішніх користувачів.

Міжмережевий екран - ідеальне місце для вбудовування засобів активного аудиту. З одного боку, і на першому, і на останньому захисному рубежі виявлення підозрілої активності по-своєму важливо. З іншого боку, МЕ здатний реалізувати скільки завгодно потужну реакцію на підозрілу активність, аж до розриву зв'язку із зовнішнім середовищем. Правда, потрібно віддавати собі звіт в тому, що з'єднання двох сервісів безпеки в принципі може створити пролом, що сприяє атак на доступність.

На міжмережевий екран доцільно покласти ідентифікацію/аутентифікацію зовнішніх користувачів, які мають доступ до корпоративних ресурсів (з підтримкою концепції єдиного входу у мережу).

В силу принципів ешелонованості оборони для захисту зовнішніх підключень зазвичай використовується двокомпонентне екранування. Первинна фільтрація (наприклад, блокування пакетів керуючого протоколу SNMP, небезпечного атаками на доступність, або пакетів з певними IP-адресами, включеними в "чорний список") здійснюється граничним маршрутизатором (див. наступний розділ), за яким розташовується так звана демілітаризована зона (мережа з помірним довірою безпеки, куди виносяться зовнішні інформаційні сервіси організації - Web, електронна пошта тощо) і основною МЕ, що захищає внутрішню частину корпоративної мережі.

Теоретично міжмережевий екран (особливо внутрішній) повинен бути багатопротокольным, однак на практиці домінування сімейства протоколів ТСП/IP настільки велике, що підтримка інших протоколів представляється надмірністю, шкідливим для безпеки (чим складніше сервіс, тим він більш вразливий).

					<i>ІТС.4КІ.0723.03-ПЗ</i>	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

Взагалі кажучи, і зовнішній, і внутрішній міжмережевий екран може стати вузьким місцем, оскільки об'єм мережевого трафіку має тенденцію швидкого зростання. Один з підходів до вирішення цієї проблеми передбачає розбиття МЕ на кілька апаратних частин і організацію спеціалізованих серверів-посередників. Основний міжмережевий екран може проводити грубу класифікацію вхідного трафіку за видами і передоручати фільтрацію відповідним посередникам (наприклад, посередника, аналізує HTTP-трафік). Вихідний трафік спочатку обробляється сервером-посередником, який може виконувати і функціонально корисні дії, такі як кешування сторінок зовнішніх Web-серверів, що знижує навантаження на мережу взагалі і основний МЕ зокрема.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є скоріше винятком, ніж правилом. Навпроти, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожний з яких підключений до Internet. У цьому випадку кожне підключення повинне захищатися своїм екраном. Точніше кажучи, можна вважати, що корпоративний зовнішній міжмережевий екран є складеним, і потрібно вирішувати задачу погодженого адміністрування (керування й аудита) усіх компонентів.

Протилежністю складовим корпоративним МЕ (або їх компонентами) є персональні міжмережеві екрани і персональні екрануючі пристрої. Перші є програмними продуктами, які встановлюються на персональні комп'ютери і захищають лише їх. Другі реалізуються на окремих пристроях і захищають невелику локальну мережу, таку як мережа домашнього офісу.

При розгортанні міжмережевих екранів слід дотримуватися розглянути нами раніше принципи архітектурної безпеки, в першу чергу подбавши про простоти і керованості, про ешелонованості оборони, а також про неможливість переходу в небезпечний стан. Крім того, слід брати до уваги не тільки зовнішні, але і внутрішні загрози.

Системи архівування і дублювання інформації

					<i>ІТС.4КІ.0723.03-ПЗ</i>	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

Організація надійної та ефективної системи архівації даних є однією з найважливіших завдань щодо забезпечення збереження інформації в мережі. У невеликих мережах, де встановлені один - два сервери, найчастіше застосовується установка системи архівації безпосередньо у вільні слоти серверів. У великих корпоративних мережах найбільш переважно організувати виділений спеціалізований сервер.

Такий сервер автоматично виконує архівування інформації з жорстких дисків для серверів і робочих станцій в зазначене адміністратором локальної обчислювальної мережі час, видаючи звіт про проведений резервному копіюванні.

Зберігання архівної інформації, що представляє особливу цінність, повинно бути організовано в спеціальному приміщенні, що охороняється. Фахівці рекомендують зберігати дублікати архівів найбільш цінних даних в іншому будинку, на випадок пожежі або стихійного лиха. Для забезпечення відновлення даних при збої магнітних дисків останнім часом найчастіше застосовуються системи дискових масивів - групи дисків, що працюють як єдиний пристрій, відповідних стандарту RAID (Redundant Arrays of Inexpensive Disks). Ці масиви забезпечують найбільш високу швидкість запису/зчитування даних, можливість повного відновлення даних і заміни вийшли з ладу дисків в "гарячому" режимі (без відключення решти дисків масиву).

Організація дискових масивів передбачає різні технічні рішення, реалізовані на декількох рівнях:

- RAID рівня 0 передбачає просте розділення потоку даних між двома або декількома дисками. Перевага такого рішення полягає в збільшенні швидкості введення/виводу пропорційно кількості задіяних у масиві дисків.
- RAID рівня 1 полягає в організації так званих "дзеркальних" дисків. Під час запису даних інформація основного диска системи

дублюється на дзеркальному диску, а при виході з ладу основного диска в роботу відразу включається "дзеркальний".

- Рівні RAID 2 і 3 передбачають створення паралельних дискових масивів, при записі на які дані розподіляються по дискам на бітовому рівні.
- Рівні RAID 4 і 5 являють собою модифікацію нульового рівня, при якому потік даних розподіляється по дисках масиву. Відмінність полягає в тому, що на рівні 4 виділяється спеціальний диск для зберігання надлишкової інформації, а на рівні 5 надлишкова інформація розподіляється по всіх дисках масиву.

Підвищення надійності та захист даних в мережі, заснована на використанні надлишкової інформації, реалізуються не тільки на рівні окремих елементів мережі, наприклад дискових масивів, але і на рівні мережесистем ОС. Наприклад, компанія Novell реалізує відмовостійкі версії операційної системи Netware - SFT (System Fault Tolerance):

- SFT Level I. Перший рівень передбачає, створення додаткових копій FAT і Directory Entries Tables, негайну верифікацію кожного знову записаного на файловий сервер блоку даних, а також резервування на кожному жорсткому диску близько 2% від обсягу диска.
- SFT Level II містила додатково можливості створення "дзеркальних дисків, а також дублювання дискових контролерів, джерел живлення і інтерфейсних кабелів.
- Версія SFT Level III дозволяє використовувати в локальній мережі дубльовані сервери, один з яких є "головним", а другий, що містить копію всієї інформації, вступає в роботу у разі виходу головного сервера з ладу.

Аналіз захищеності

Сервіс аналізу захищеності призначений для виявлення вразливих місць з метою їх оперативної ліквідації. Сам по собі цей сервіс ні від чого не

					ІТС.4КІ.0723.03-ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

захищає, але допомагає виявити (і усунути) прогалини в захисті раніше, ніж їх може використати зловмисник. В першу чергу, маються на увазі не архітектурні (їх ліквідувати складно), а "оперативні" проломи, що з'явилися в результаті помилок адміністрування або із-за неуваги до оновлення версій програмного забезпечення.

Системи аналізу захищеності (звані також сканерами захищеності), як і розглянуті вище засоби активного аудиту, засновані на накопиченні та використанні знань. В даному випадку маються на увазі знання про прогалини в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати.

Відповідно, ядром таких систем є база вразливих місць, яка визначає доступний діапазон можливостей і вимагає практично постійної актуалізації.

У принципі, можуть виявлятися проломи самої різної природи: наявність шкідливого ПЗ (зокрема, вірусів), слабкі паролі користувачів, невдало сконфігуровані операційні системи, небезпечні мережеві сервіси, невстановлені латки, уразливості в програмах і т. д. Однак найбільш ефективними є мережеві сканери (очевидно, в силу домінування сімейства протоколів TCP/IP), а також антивірусні засоби[14]. Антивірусний захист ми зараховуємо до засобів аналізу захищеності, не вважаючи її окремим сервісом безпеки.

Сканери можуть виявляти вразливі місця як шляхом пасивного аналізу, тобто вивчення конфігураційних файлів, задіяних портів і т. п., так і шляхом імітації дій атакуючого. Деякі знайдені вразливі місця можуть усуватися автоматично (наприклад, лікування заражених файлів), про інших повідомляється адміністратору.

Контроль, забезпечуваний системами аналізу захищеності, носить реактивний, запізнілий характер, він не захищає від нових атак, проте слід пам'ятати, що оборона повинна бути ешелонованою, і в якості одного з рубежів контроль захищеності цілком адекватний. Відомо, що переважна

					ІТС.4КІ.0723.03-ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

більшість атак носить рутинний характер; вони можливі лише тому, що відомі проломи в захисті роками залишаються неусунення.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 2

Фізичний захист інформації включає заходи, спрямовані на захист фізичного середовища, приміщень, обладнання і носіїв інформації. Це важлива складова частина загальної стратегії захисту інформації, оскільки незаконний фізичний доступ до систем і даних може призвести до серйозних наслідків, включаючи крадіжку, втрату, розкриття або пошкодження інформації.

Загальний висновок з тексту щодо апаратних засобів захисту інформації полягає в тому, що вони виконують важливі функції для забезпечення інформаційної безпеки в комп'ютерних системах. Апаратні засоби включають пристрої для ідентифікації користувачів, шифрування інформації, захисту від несанкціонованого доступу, знищення інформації на носіях та сигналізації при спробах несанкціонованої дії. Вони є важливою складовою частиною комплексного підходу до захисту даних і можуть сприяти покращенню безпеки в організації.

Програмні засоби захисту інформації є спеціальними програмами, які включаються до складу програмного забезпечення КМ (комп'ютерної системи) для виконання захисних функцій.

Основні програмні засоби захисту інформації включають програми ідентифікації і аутентифікації користувачів, програми розмежування доступу користувачів, програми шифрування інформації та програми захисту інформаційних ресурсів від несанкціонованої зміни, використання та копіювання.

Ідентифікація означає розпізнавання унікального імені суб'єкта КМ, а аутентифікація підтверджує достовірність цього суб'єкта.

Поміж інших програмних засобів захисту інформації можна виділити програми знищення залишкової інформації, програми аудиту подій безпеки, програми імітації роботи з порушником та програми тестового контролю захищеності.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги програмних засобів захисту інформації включають простоту тиражування, гнучкість, простоту застосування і можливості розвитку шляхом внесення змін.

Недоліки програмних засобів захисту інформації включають зниження ефективності комп'ютерної системи, більш низьку продуктивність порівняно з апаратними засобами захисту, залежність від обходу злоумисниками та можливість зміни програмних засобів в процесі експлуатації.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3.

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Організаційно-правове забезпечення захисту інформації

На підприємстві розроблені наступні заходи щодо захисту інформації:

- укладено договір про охорону приміщень і території (діє пропускний режим);
- розроблений режим і правила протипожежної безпеки;
- режим відеоспостереження поверхів;
- розроблені посадові інструкції службовців, розмежовують їх права та обов'язки;
- додаткові угоди до трудових договорів працівників про нерозголошення ними конфіденційної інформації, що регламентують відповідальність в області захисту інформації;
- інструкції з охорони периметра, по експлуатації системи охоронної сигналізації та відеоспостереження;
- положення про конфіденційний документообіг;
- опис технологічного процесу обробки КІ;
- встановлена антивірусна системи захисту на АРМ;
- розмежований доступ до АРМ паролями.

Правове забезпечення системи захисту конфіденційної інформації включає в себе комплекс внутрішньої нормативно-організаційної документації, в яку входять такі документи підприємства, як[4]:

					ІТС.4КІ.0723.03-ПЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	РОЗДІЛ 3 МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ			Лім.	Арк.	Акрушів
Розроб.		Берест Р.Ю.								
Керівник		Матієвський В.В.							45	2
Реценз.		Козуб Ю.Г.						ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.										
Зав. каф.		Семенов М.А..								

- Статут;
- колективний трудовий договір;
- трудові договори з працівниками підприємства;
- правила внутрішнього розпорядку службовців підприємства;
- посадові обов'язки керівників, фахівців і службовців

підприємства.

- інструкції користувачів інформаційно-обчислювальних мереж та баз даних;
- інструкції співробітників, відповідальних за захист інформації;
- пам'ятка співробітника про збереження комерційної або іншої таємниці;
- договірні зобов'язання.

Не заглиблюючись у зміст перелічених документів, можна сказати, що у всіх з них, залежно від їх основного нормативного або юридичної призначення, зазначаються вимоги, норми і правила щодо забезпечення необхідного рівня інформаційної захищеності підприємства, звернені, насамперед, до персоналу і керівництва.

Правове забезпечення дає можливість врегулювати багато спірні питання, що неминуче виникають у процесі інформаційного обміну на самих різних рівнях - від мовного спілкування до передачі даних в комп'ютерних мережах. Крім того, утворюється юридично оформлена система адміністративних заходів, що дозволяє застосовувати стягнення або санкції до порушників внутрішньої політики безпеки, а також встановлювати досить чіткі умови щодо забезпечення конфіденційності відомостей, що використовуються чи формуються при співробітництві між суб'єктами економіки, виконання ними договірних зобов'язань, здійснення спільної діяльності і т. п. При цьому сторони, які не виконують ці умови, несуть відповідальність в межах, передбачених як відповідними пунктами між

					ІТС.4КІ.0723.03-ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		

сторонніх документів (договорів, угод, контрактів тощо), так і російським законодавством.

Основними об'єктами захисту є:

- АРМ співробітників;
- сервер локальної мережі;
- конфіденційна інформація (документи);
- кабінети генерального директора, головного інженера та

головного технолога;

- кабінети з конфіденційною документацією.

У додатку А представлено План заходів із заходів із захисту інформації в мережі підприємства.

3.2 Захист інформації в корпоративній мережі на рівні операційної системи

Windows Server має засоби забезпечення безпеки, вбудовані в операційну систему. Нижче розглянуті найбільш значущі з них[14].

Стеження за діяльністю мережі.

Windows Server дає багато інструментальних засобів для спостереження за мережевою діяльністю і використанням мережі. ОС дозволяє:

- переглянути сервер і побачити, які ресурси він використовує;
- побачити користувачів, підключених до сервера і побачити, які файли у них відкриті;
- перевірити дані у журналі безпеки;
- перевірити записи в журналі подій;
- вказати, про які помилки адміністратор повинен бути попереджений, якщо вони відбудуться.

Початок сеансу на робочій станції

					ITC.4KI.0723.03-ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

Всякий раз, коли користувач починає сеанс на робочій станції, екран початку сеансу запитує ім'я користувача, пароль і домен. Потім робоча станція посилає ім'я користувача і пароль домену для ідентифікації. Сервер у домені перевіряє ім'я і пароль користувача в базі даних облікових карток користувачів домену. Якщо ім'я користувача та пароль ідентичні даними в обліковій картці, сервер повідомляє робочу станцію про початку сеансу. Сервер завантажує іншу інформацію при початку сеансу користувача, як наприклад установки користувача, свій каталог і змінні середовища.

За замовчуванням не всі облікові картки в домені дозволяють входити в систему. Тільки картками груп адміністраторів, операторів сервера, операторів управління печаткою, операторів керування обліковими картками та операторів керування резервним копіюванням дозволено це робити.

Для всіх користувачів мережі підприємства передбачено своє ім'я і пароль (детальніше про це розповідається в наступному розділі ВКР).

Облікові картки користувачів

Кожен клієнт, який використовує мережу, має облікову картку користувача в домені мережі. Облікова картка користувача містить інформацію про користувача, що включає ім'я, пароль і обмеження по використанню мережі, що накладаються на нього. Облікові картки дозволяють згрупувати користувачів, які мають аналогічні ресурси, групи; групи полегшують надання прав і дозволів на ресурси, досить зробити тільки одну дію, що дає права чи дозволу всій групі.

Додаток показує вміст облікової картки користувача.

Журнал подій безпеки

Windows 2003 Server дозволяє визначити, що увійде в ревізію і буде записано в журнал подій безпеки всякий раз, коли виконуються певні дії або здійснюється доступ до файлів. Елемент ревізії показує виконану дію користувача, який виконав його, а також дату і час дії. Це дозволяє контролювати як успішні, так і невдалі спроби будь-яких дій.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

Журнал подій безпеки для умов підприємства є обов'язковим, оскільки у разі спроби злому мережі можна буде відстежити джерело.

Насправді протоколювання здійснюється лише стосовно підозрілих користувачів і подій. Оскільки якщо фіксувати всі події, обсяг реєстраційної інформації, швидше за все, буде рости занадто швидко, а її ефективний аналіз стане неможливим. Стеження важлива в першу чергу як профілактичний засіб. Можна сподіватися, що багато утримаються від порушень безпеки, знаючи, що їхні дії фіксуються.

Права користувача

Права користувача визначають дозволені типи дій для цього користувача. Дії, що регулюються правом, належать вхід в систему на локальний комп'ютер, вимикання, встановлення часу, копіювання і відновлення файлів сервера і виконання інших завдань.

В домені Windows 2003 Server права надаються та обмежуються на рівні домену; якщо група знаходиться безпосередньо в домені, учасники мають право у всіх первинних і резервних контролерах домену.

Для кожного користувача підприємства обов'язково встановлюються свої права доступу до інформації, дозвіл на копіювання та відновлення файлів.

Установка пароля й політика облікових карток

Для домену визначені всі аспекти політики пароля: мінімальна довжина пароля (6 символів), мінімальний і максимальний вік пароля і винятковість пароля, який захищає користувача від зміни його пароля на той пароль, який користувач використовував недавно.

Дається можливість також визначити й інші аспекти політики облікових карток:

- повинна відбуватися блокування облікової картки;
- чи повинні користувачі насильно відключатися від сервера після закінчення годин початку сеансу;

					ІТС.4КІ.0723.03-ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

- чи повинні користувачі мати можливість входу в систему, щоб змінити свій пароль.

Коли дозволена блокування облікової картки, тоді облікова картка блокується у разі декількох безуспішних спроб початку сеансу користувача, і не більш, ніж через певний період часу між будь-якими двома безуспішними спробами початку сеансу. Облікові картки, які заблоковані, не можуть бути використані для входу в систему.

Якщо користувачі примусово відключаються від серверів, коли час його сеансу минув, то вони отримують попередження як раз перед кінцем встановленого періоду сеансу. Якщо користувачі не відключаються від мережі, то сервер зробить відключення примусово. Однак відключення користувача від робочої станції не відбудеться. Годинник сеансу на підприємстві не встановлено, так як в успішній діяльності зацікавлені всі працівники і часто деякі залишаються працювати понаднормово або у вихідні дні.

Якщо від користувача потрібно змінити пароль, то, коли він цього не зробив за прострочений пароль, він не зможе змінити свій пароль. При простроченні пароля користувач повинен звернутися до адміністратора системи за допомогою у зміні пароля, щоб мати можливість знову входити в мережу. Якщо користувач не входив в систему, а час зміни пароля підійшло, то він буде попереджений про необхідність зміни, як тільки він буде входити.

Файлова система EFS

Windows надає можливість ще більше захистити зашифровані файли і папки на томах NTFS завдяки використанню файлової системи із шифруванням (Encrypting File System). При роботі в середовищі Windows 2000 можна працювати тільки з тими томами, на які є права доступу.

При використанні файлової системи із ШИФРУВАННЯМ можна файли і папки, дані яких будуть зашифровані з допомогою пари ключів. Будь-який користувач, який захоче отримати доступ до певного файлу, повинен володіти особистим ключем, з допомогою якого дані файлу

					ІТС.4КІ.0723.03-ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

розшифровуватися. Система EFS так само забезпечує схему захисту файлів у середовищі Windows. Однак, на підприємстві не використовується ця можливість, так як при використанні шифрування продуктивність роботи системи знижується.

У додатку Б представлено основні методи захисту інформації.

3.3 Захист інформації від несанкціонованого доступу

Вище вже були зазначені організаційно-правові аспекти захисту інформації від несанкціонованого доступу і можливості Windows 2000 в цьому плані. Тепер зупинюся трохи докладніше на інших аспектах.

Інформація, що циркулює в корпоративній мережі досить різноманітна. Всі інформаційні ресурси розділені на три групи:

Мережеві ресурси загального доступу;

Інформаційні ресурси файлового сервера;

Інформаційні ресурси СУБД.

Кожна група містить ряд найменувань інформаційних ресурсів, які в свою чергу мають індивідуальний код, рівень доступу, розташування, власника і т. п.

Ця інформація важлива для підприємства та його клієнтів, тому вона повинна мати гарний захист.

Електронні ключі

Всі комп'ютери, що працюють з відомостями, що становлять комерційну таємницю, обладнані додатковими програмно-апаратними комплексами.

Такі комплекси являють собою сукупність програмних і апаратних засобів захисту інформації від несанкціонованого доступу.

Апаратна частина, подібних комплексів так званий електронний замок являє собою електронну плату, встановлювану в один із слотів комп'ютера і забезпечені інтерфейсом для підключення зчитувача електронних ключів

					ІТС.4КІ.0723.03-ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

таких типів як: Smart Card, Touch Memory, Proximity Card, eToken. Типовим набором функцій, що надаються такими електронними замками, є:

- реєстрації користувачів комп'ютера та призначення їм персональних ідентифікаторів (імен та/або електронних ключів) і паролів для входу в систему;
- запит персонального ідентифікатора і пароля користувача при завантаженні комп'ютера. Запит здійснюється апаратною частиною до завантаження ОС;
- можливість блокування входу в систему зареєстрованого користувача;
- ведення системного журналу, в якому реєструються події, що мають відношення до безпеки системи;
- контроль цілісності файлів на жорсткому диску;
- контроль цілісності фізичних секторів жорсткого диска;
- апаратну захист від несанкціонованої завантаження операційної системи з гнучкого диска, CD-ROM або USB портів;
- можливість спільної роботи з програмними засобами захисту від несанкціонованого доступу.

Опикунська захист даних

На підприємстві використовується такий варіант захисту інформації як опикунська захист даних. Піклувальник - це користувач, якому надано привілеї або права доступу до файлових ресурсів.

Кожен співробітник має одну з восьми різновидів прав:

- Read - право Читання відкритих файлів;
- Write - право Запису у відкриті файли;
- Open - право Відкриття існуючого файлу;
- Create - право Створення (і одночасно відкриття) нових файлів;
- Delete - право на Видалення існуючих файлів;
- Parental - Батьківські права:

- право Створення, перейменування, Видалення підкаталогів каталогу;
- право Встановлення піклувальників та прав в каталозі;
- право Встановлення піклувальників та прав у підкаталозі;
- Search - право Пошуку каталогу;
- Modify - право Модифікації файлових атрибутів.

Для запобігання випадкових змін або вилучення окремих файлів усіма працівниками використовується захист атрибутами файлів. Такий захист застосовується щодо інформаційних файлів загального користування, які зазвичай читаються багатьма користувачами. Захист даних використовуються чотири файлових атрибута:

- Запис-читання,
- Тільки читання,
- Поділюваний,
- Нерозривний.

Паролі

Як я вже вказував, всі комп'ютери на підприємстві захищені паролем.

Оскільки на всіх комп'ютерах організації встановлений Microsoft Windows 2000 і Windows Server 2003, то використовується захист паролем операційної системи, яка встановлюється адміністратором в BIOS, так як найважливішу роль у запобіганні несанкціонованого доступу до даних комп'ютера відіграє саме захист BIOS.

Модифікація, знищення BIOS персонального комп'ютера можливе в результаті несанкціонованого скидання або роботи шкідливих програм, вірусів.

В залежності від моделі комп'ютера захист BIOS забезпечується:

- установкою перемикача, розташованого на материнській платі, у положення, що виключає модифікацію BIOS (проводиться службою технічної підтримки підрозділи автоматизації);
- установкою адміністративного пароля ПЗ SETUP.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

Захист BIOS від несанкціонованого скидання забезпечується опечатуванням корпусу комп'ютера захисної голографічною наклейкою.

Використовуються два типи паролів доступу: адміністративні та користувача.

При встановленні адміністративного і користувальницького пароля слід керуватися наступними правилами:

- пароль користувач комп'ютера вибирає і провадить одноособово (не менше 6-ти символів). Адміністратора інформаційної безпеки забороняється дізнаватися пароль користувача.
- адміністративний пароль (не менше 8-ми символів) вводиться адміністратором інформаційної безпеки. Адміністратора інформаційної безпеки забороняється повідомляти адміністративний пароль користувача.
- У тому випадку, якщо комп'ютер обладнаний апаратно-програмним засобом захисту від НСД, яке забороняє завантаження ОС без пред'явлення користувача персонального ідентифікатора, пароль допускається не встановлювати.
- При позитивному результаті перевірки достовірності пред'явленого користувачем пароля:
 - система управління доступом надає користувачеві закріплені за ним права доступу;
 - користувач реєструється вбудованими засобами реєстрації (якщо вони є).

Контроль доступу в Інтернет

Особливу увагу слід приділяти доступу працівників підприємства до мережі Інтернет.

Раніше доступ до мережі Internet здійснювався зі спеціалізованого робочого місця, званого Інтернет-кіоском. Інтернет-кіоск не був підключений до корпоративної мережі підприємства.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

У підрозділі, що здійснював експлуатацію Інтернет-кіоску, велися:

- журнал обліку робіт у мережі Internet, в якому відображалися: ПІБ користувача, дата, час початку робіт, тривалість робіт, мета робіт, ресурси, що використовуються, підпис;
- журнал допуску, в якому відображалися: ПІБ користувача, задачі, для вирішення яких він допускається до роботи в мережі Internet, час проведення робіт і максимальна тривалість, підпис керівника.

Але від цієї практики згодом відмовилися. Зараз всі комп'ютери локальної мережі мають вихід в Інтернет.

Зростання спектру і обсягів послуг, що тягнуть за собою потребу підрозділів в інформаційному обміні з зовнішніми організаціями, а також необхідність надання віддаленого доступу до інформації через публічні канали зв'язку, значно підвищують ризики несанкціонованого доступу, вірусної атаки і т. п.

3.4 Антивірусний захист

Враховуються фактори ризику

Віруси можуть проникати в машину різними шляхами (через глобальну мережу, через заражену дискету або флешку). Наслідки їх проникнення вельми неприємні: від руйнування файлу до порушення працездатності всього комп'ютера. Достатньо всього лише одного зараженого файлу, щоб заразити всю наявну на комп'ютері інформацію, а далі заразити всю корпоративну мережу.

При організації системи антивірусного захисту на підприємстві враховувалися наступні фактори ризику:

- обмежені можливості антивірусних програм

Можливість створення нових вірусів з орієнтацією на протидію конкретним антивірусним пакетів і механізмам захисту, використання вразливостей системного та прикладного ПЗ призводять до того, що навіть

					ІТС.4КІ.0723.03-ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

тотальне застосування антивірусних засобів з актуальними антивірусними базами не дає гарантованого захисту від загрози вірусного зараження, оскільки можлива поява вірусу, процедури захисту від якого ще не додані новітні антивірусні бази.

- висока інтенсивність виявлення критичних вразливостей в системному ПЗ

Наявність нових неусунутих критичних вразливостей в системному ПЗ, створює канали масового розповсюдження нових вірусів по локальних і глобальних мереж. Включення до складу вірусів «шпигунських» модулів, що забезпечують можливість віддаленого управління комп'ютером з максимальними привілеями, створює не тільки ризики масового відмови в обслуговуванні, але і ризики прямих розкрадань шляхом несанкціонованого доступу в автоматизовані банківські системи.

- необхідність попереднього тестування оновлень системного та антивірусного ПЗ

Установка оновлень без попереднього тестування створює ризики несумісності системного, прикладного та антивірусного ПО і може призводити до порушень у роботі. У той же час тестування призводить до додаткових затримок в установці оновлень і відповідно збільшує ризики вірусного зараження.

- різноманітність та кроссплатформеність використовуються в автоматизованих системах технічних засобів і програмного забезпечення

Можливість роботи окремих типів вірусів на різних платформах, здатність до розмноження вірусів з використанням корпоративних поштових систем або обчислювальних мереж, відсутність антивірусних продуктів для деяких конкретних платформ роблять у ряді випадків неможливим чи неефективним застосування антивірусного ПЗ.

- широка доступність сучасних мобільних засобів зв'язку, пристроїв зберігання і носіїв інформації великої ємності

					ІТС.4КІ.0723.03-ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

Сучасні мобільні засоби зв'язку дозволяють недобросовісним працівникам здійснити несанкціоноване підключення автоматизованого робочого місця до мережі Інтернет, створивши тим самим пролом в периметрі безпеки корпоративної мережі і піддавши її інформаційні ресурси ризику масового зараження новим комп'ютерним вірусом. Наявність доступних компактних пристроїв зберігання і перенесення великих об'ємів інформації створює умови для несанкціонованого використання таких пристроїв і носіїв в особистих виробничих цілях. Несанкціоноване копіювання на комп'ютери підприємства інформації, отриманої з неперевірених джерел, істотно збільшує ризики вірусного зараження.

- необхідність кваліфікованих дій з відбиття вірусної атаки

Некваліфіковані дії по відображенню вірусної атаки можуть призводити до поглиблення наслідків зараження, часткової або повної втрати критичної інформації, неповної ліквідації вірусного зараження або навіть розширення вогнища зараження.

- необхідність планування заходів по виявленню наслідків вірусної атаки і відновлення ураженої інформаційної системи

У разі безпосереднього впливу вірусу на автоматизовану банківську систему, або при проведенні некваліфікованих лікувальних заходів може бути втрачена інформація або спотворене програмне забезпечення.

В умовах дії зазначених факторів тільки прийняття жорстких комплексних заходів безпеки з усіх можливих видів загроз дозволить контролювати постійно зростаючі ризики повної або часткової зупинки бізнес процесів в результаті вірусних заражень.

Висновки до розділу 3

Можна зробити наступні висновки:

Організаційно-правове забезпечення захисту інформації є важливим етапом в захисті корпоративних мереж. Для успішного забезпечення безпеки

					ІТС.4КІ.0723.03-ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

необхідно розробляти політики, стандарти та процедури, а також визначати відповідальних осіб за безпеку інформації.

Захист інформації в корпоративній мережі на рівні операційної системи має велике значення. Для цього необхідно встановлювати та налаштовувати заходи безпеки, такі як автентифікація, авторизація, контроль доступу та моніторинг системи.

Захист інформації від несанкціонованого доступу є критичним завданням у корпоративних мережах. Необхідно використовувати різноманітні технології, такі як брандмауери, віртуальні приватні мережі (VPN), шифрування даних та системи виявлення вторгнень (IDS) для забезпечення безпеки.

Антивірусний захист є важливою складовою безпеки інформації у корпоративних мережах. Він полягає в установці та оновленні антивірусного програмного забезпечення на всіх комп'ютерах та серверах, регулярних перевірок на наявність вірусів та шкідливого програмного забезпечення.

Загалом, захист інформації у корпоративних мережах вимагає комплексного підходу, поєднання організаційних, правових та технічних заходів.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВОК

Прогрес подарував людству безліч досягнень, але той же прогрес породив і безліч проблем. Людський розум, вирішуючи одні проблеми, неодмінно стикається при цьому з іншими, новими. Вічна проблема - захист інформації. На різних етапах свого розвитку людство вирішувало цю проблему з властивою для даної епохи характерна. Винахід комп'ютера і подальший бурхливий розвиток інформаційних технологій у другій половині 20 століття зробили проблему захисту інформації настільки актуальною і гострою, наскільки актуальна сьогодні інформатизація всього суспільства. Головна тенденція, що характеризує розвиток сучасних інформаційних технологій - зростання кількості комп'ютерних злочинів і пов'язаних з ними розкрадання конфіденційної та іншої інформації, а також матеріальних втрат.

Сьогодні, напевно, ніхто не зможе з упевненістю назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних з несанкціонованим доступом до інформації. Це пояснюється, насамперед, небажанням постраждалих компаній оприлюднити інформацію про свої втрати, а також тим, що не завжди втрати від розкрадання інформації можна точно оцінити в грошовому еквіваленті.

Причин активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат досить багато, істотними з них є:

- перехід від традиційної "паперової" технології зберігання і передачі інформації на електронну та недостатнє при цьому розвиток технології захисту інформації в таких технологіях;
- об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

					ІТС.4КІ.0723.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	ВИСНОВОК	Літ.	Арк.	Акрушів	
Розроб.		Берест Р.Ю.							
Керівник		Матієвський В.В.					59	2	
Реценз.		Козуб Ю.Г.				ЛНУ Кафедра ІТС, Гр.4КІ			
Н. Контр.									
Зав. каф.		Семенов М.А..							

- збільшення складності програмних засобів і пов'язане з цим зменшення їх надійності і збільшенням числа вразливостей.

Комп'ютерні мережі, в силу своєї специфіки, просто не зможуть нормально функціонувати і розвиватися, ігноруючи проблеми захисту інформації.

У першій главі моєї кваліфікаційної роботи були розглянуті різні види загроз та ризиків. Загрози безпеки діляться на природні і штучні, а штучні в свою чергу поділяються на ненавмисні і навмисні.

До найпоширеніших загроз відносяться помилки користувачів комп'ютерної мережі, внутрішні відмови мережі або підтримуючої інфраструктури, програмні атаки і шкідливе програмне забезпечення.

Заходи забезпечення безпеки комп'ютерних мереж підрозділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні, технічні (апаратно-програмні).

У другій главі ВКР докладно розглянуто деякі з фізичних, апаратних і програмних засобів захисту. До сучасним програмним засобам захисту інформації відносяться криптографічні методи, шифрування дисків, ідентифікація і аутентифікація користувача. Для захисту локальної або корпоративної мережі від атак з глобальної мережі застосовують спеціалізовані програмні засоби: брандмауери або проксі-сервери. брандмауери – це спеціальні проміжні сервери, які інспектують і фільтрують весь що проходить через них трафік мережевого/ транспортного рівнів. Проксі-сервер – це сервер-посередник, всі звернення з локальної мережі в глобальну відбуваються через нього.

Організація надійної та ефективної системи архівації даних також є однією з найважливіших завдань щодо забезпечення збереження інформації в мережі. Для забезпечення відновлення даних при збої магнітних дисків останнім часом найчастіше застосовуються системи дискових масивів - групи дисків, що працюють як єдиний пристрій, відповідних стандарту RAID.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

Для виявлення вразливих місць з метою їх оперативної ліквідації призначений сервіс аналізу захищеності. Системи аналізу захищеності (звані також сканерами захищеності), як і розглянуті вище засоби активного аудиту, засновані на накопиченні та використанні знань. В даному випадку маються на увазі знання про прогалини в захисті: про те, як їх шукати, наскільки вони серйозні і як їх усувати.

У третьому розділі розглянуто методи і засоби захисту інформації в телекомунікаційних мережах підприємств. Докладно розглянуто організаційно-правову забезпечення захисту, докладно розглянуто захисні можливості операційної системи Windows Server, яка використовується на підприємстві. Дуже важливо захистити корпоративну мережу від несанкціонованого доступу. Для цього на підприємстві використовуються електронні ключі, організована опікунська захист даних, що встановлені паролі, здійснюється контроль доступу в Інтернет.

Щоб виключити зараження корпоративної мережі комп'ютерними вірусами, використовує пакет антивірусних

Проаналізувавши доступну інформацію про організації захисту корпоративної мережі, можливо зробити наступний висновок: Фахівці підприємства створили грамотну і надійно працюючу систему захисту. Мені складно що-небудь пропонувати для вдосконалення її технологій. Зрозуміло, можна виділити найбільш дієві заходи захисту інформації в мережах це:

- розмежування повноважень;
- використання ліцензійного ПЗ;
- ідентифікація і аутентифікація користувачів;
- резервне копіювання;
- гарне антивірусне програмне забезпечення;
- регулярне оновлення антивірусної бази.

У цьому випадку ступінь захисту інформації значно зросте.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cookbooks 2. 20/20 Cookbooks Presents: 85 Fat-Burning Diet Meal Recipes to Help You Lose Weight Faster and Stay Full Longer. Not Avail, 2018. 104 p.
2. Fruhlinger J. What is network security? Definition, methods, jobs & salaries. CSO Online. URL:
<https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html> (дата звернення: 03.05.2023).
3. Tanenbaum A. S., Wetherall D. J. Computer Networks 5th By Andrew S. Tanenbaum (International Economy Edition). Prentice Hall, Indian International Ed., 2010. 960 p.
4. Андреев Б. В. Захист прав і свобод людини і громадянина в інформаційній сфері // Системи безпеки, № 1, 2002. С. 10-13
5. Безпека мережі (мережева безпека) - що це і для чого, як працює? ESET. ESET. URL:
<https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/> (дата звернення: 15.06.2023).
6. Бондар, О. Р., & Верес, Л. А. . Розробка рекомендацій щодо забезпечення безпеки в мережі підприємства на основі методів якості обслуговування. збірник матеріалів міжнародної науково-технічної конференції «перспективи телекомунікацій». вилучено із <http://conferenc.its.kpi.ua/proc/article/view/200885> 2020
7. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков – К.: Видавнича група BVH, 2009. – 608 с.

					ІТС.4КІ.0721.03-ПЗ						
Змн.	Арк.	№ докум.	Підпис	Дата							
Розроб.		Берест Р.Ю.			СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ			Літ.	Арк.	Акрушіє	
Керівник		МатієвськийВ.В.								62	7
Реценз.		Козуб Ю.Г.						ЛНУ Кафедра ІТС, Гр.4КІ			
Н. Контр.											
Зав. каф.		Семенов М.А..									

8. Інформаційна безпека підприємства: методи захисту від головних загроз - FSG. FSG. URL: <https://group-fs.com/informaczijna-bezpeka-pidpryyemstva-metody-zahystu-vid-golovnyh-zagrozh/> (дата звернення: 01.06.2023).

9. Комп'ютерні мережі частина 1 навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с

10. Остапов С. Е. Основи криптографії: навчальний посібник / С. Е. Остапов, Л. О. Валь. – Чернівці: Книги–XXI, 2008. – 188 с

11. Стрихалюк Б. М. Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с

12. Учасники проектів Вікімедіа. Безпека мережі – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Безпека_мережі (дата звернення: 15.04.2023).

13. Інформаційна безпека: види загроз і методи їх усунення - datami. datami. URL: <https://datami.ua/informatsijna-bezpeka-vidi-zagrozh-i-metodi-yih-usunennya/> (дата звернення: 12.04.2023).

14. У чому різниця між Windows і Windows Server? / як. Кращі уроки по веб-розробці. URL: <https://ua.phhsnews.com/articles/howto/whats-the-difference-between-windows-and-windows-server.html> (дата звернення: 02.03.2023).

					ІТС.4КІ.0723.03-ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

Додаток А План заходів із захисту інформації в мережі підприємства

1. Проведення аудиту безпеки мережі для виявлення потенційних загроз і вразливостей.
2. Встановлення брандмауера для контролю трафіку та фільтрації небажаного або шкідливого трафіку.
3. Використання інтрузійних виявлення і запобігання (IDS/IPS) для виявлення та запобігання незвичайній або підозрілій активності.
4. Встановлення системи моніторингу безпеки, яка відстежує події в мережі та виявляє аномалії.
5. Використання криптографічних пристроїв та протоколів для шифрування та захисту конфіденційної інформації.
6. Встановлення системи резервного копіювання та відновлення даних для захисту від втрати даних внаслідок аварій або кібератак.
7. Використання системи аутентифікації та управління доступом для обмеження доступу до ресурсів мережі тільки авторизованим користувачам.
8. Використання комплексних паролів та регулярна зміна паролів для запобігання несанкціонованому доступу.
9. Впровадження системи мультифакторної аутентифікації для підвищення рівня безпеки при вході в систему.
10. Налаштування системи автоматичних оновлень для оперативного отримання патчів безпеки та виправлень програмних вразливостей.
11. Регулярне оновлення антивірусного програмного забезпечення та виконання сканування системи для виявлення шкідливих програм.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		

12. Встановлення політики безпеки, яка включає правила щодо використання паролів, обмеження доступу до ресурсів та інші вимоги безпеки.
13. Навчання працівників з питань безпеки інформації, включаючи небезпеки фішингу та соціального інжинірингу.
14. Впровадження системи моніторингу інформаційної безпеки, яка виявляє незвичайну або підозрілу активність інсайдерів.
15. Забезпечення фізичної безпеки приміщень, де розташовані сервери та мережеві пристрої.
16. Використання захищених бездротових мереж з шифруванням для уникнення несанкціонованого доступу.
17. Встановлення системи регулярного аудиту мережі для перевірки відповідності безпечним стандартам та виявлення можливих проблем.
18. Впровадження системи виявлення та реагування на інциденти (IR), яка дозволяє вчасно реагувати на кібератаки та відновлювати безпеку.
19. Встановлення фізичних бар'єрів, таких як камери відеоспостереження та контроль доступу, для захисту серверних приміщень та інфраструктури мережі.
20. Проведення регулярного тестування на проникнення для оцінки безпеки мережі та виявлення можливих вразливостей.

Додаток Б Основні методи захисту інформації в корпоративній мережі на основі Windows

1. Використання брандмауера Windows: Встановлення та налагодження брандмауера Windows для контролю трафіку в мережі, фільтрації пакетів і блокування небажаного або шкідливого трафіку.
2. Встановлення оновлень та патчів безпеки: Регулярне оновлення операційної системи Windows і програмного забезпечення на всіх комп'ютерах мережі з метою закриття вразливостей і запобігання експлойтації зловмисниками.
3. Використання антивірусного програмного забезпечення: Установка та оновлення антивірусного програмного забезпечення на всіх комп'ютерах для виявлення та блокування шкідливих програм і загроз.
4. Використання системи аутентифікації: Встановлення системи аутентифікації, такої як Active Directory, для управління користувачами, групами, політиками паролів і обмежень доступу до ресурсів.
5. Впровадження політики паролів: Встановлення правил щодо складності паролів, регулярної зміни паролів і обмежень на спроби введення паролів з метою запобігання несанкціонованому доступу.
6. Використання групових політик: Використання групових політик для централізованого управління налаштуваннями безпеки на комп'ютерах мережі, включаючи політики паролів, блокування USB-портів і обмеження програм.
7. Встановлення системи моніторингу безпеки: Використання системи моніторингу подій і журналів безпеки Windows для виявлення незвичайної або підозрілої активності, спроб вторгнення або зловживання правами доступу.
8. Захист від вторгнень: Використання системи виявлення і запобігання вторгнень (Intrusion Detection and Prevention System - IDS/IPS) для

автоматичного виявлення та блокування незвичайних або шкідливих активностей в мережі.

9. Захист від фішингу та соціального інжинірингу: Проведення навчання співробітників з питань безпеки, включаючи виявлення фішингових атак, підозрілих посилань та шкідливих вкладень.

10. Резервне копіювання та відновлення даних: Встановлення системи резервного копіювання і відновлення даних для захисту від втрати даних внаслідок аварій, кібератак або помилкових вилучень.

11. Обмеження прав доступу: Встановлення обмежень прав доступу до ресурсів, файлів і папок залежно від ролей та обов'язків користувачів.

12. Використання шифрування даних: Використання шифрування для захисту конфіденційних даних під час передачі і зберігання.

					ІТС.4КІ.0723.03-ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		