

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захисту інфраструктури локальної
мережі будівельної компанії»

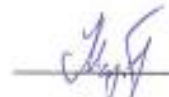
Виконав студент 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Литвинчук В.С.

Керівник старший викладач кафедри комп'ютерних
наук

 Петросян Р. В.

Рецензент ВО завідувача кафедри комп'ютерних наук,
к.т.н.

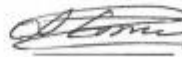
 Граф М. С.

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Литвинюк Вадим Сергійович

Тема роботи: «Проект захисту інфраструктури локальної мережі будівельної компанії»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є захист інфраструктури локальної мережі компанії.

Предмет дослідження – використання різноманітних систем та методів захисту інформації в компанії.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2022- 11.03.2022	
2	Аналіз літературних джерел	11.03.2022- 13.03.2022	
3	Аналіз об'єкта дослідження	13.03.2022- 20.04.2022	
4	Аналіз оброблюваних даних компанії	20.04.2022- 04.05.2022	
5	Розробка структурної моделі	04.05.2022- 12.05.2022	
6	Проектування розміщення вузлів мережі	12.05.2022- 01.06.2022	
7	Налаштування серверного сегменту комп'ютерної мережі	01.06.2022- 04.06.2022	
8	Реалізація моделі комп'ютерної мережі за допомогою Packet Tracer	04.06.2022- 06.06.2022	
9	Оформлення пояснювальної записки	06.06.2022- 16.06.2022	
10	Захист	Згідно з розкладом	

Студент  Литвинюк В.С.

Керівник  Петросян Р. В.

АНОТАЦІЯ

Дипломна робота містить 102 сторінок тексту, 26 рисунків, 4 таблиці посилання на 12 літературних джерел.

Метою роботи є проектування локальної комп'ютерної мережі будівельної компанії та розробка рекомендації для оптимізації процесів забезпечення інформаційної безпеки для неї.

Результатом виконання кваліфікаційної роботи є розробка локальної комп'ютерної мережі будівельної компанії.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМУТАТОР, МАРШРУТИЗАТОР, МЕРЕЖЕВА АРХІТЕКТУРА, ОБ'ЄКТ ЗАХИСТУ, ОРГАНІЗАЦІЯ ЗАХИСТУ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СЕРВЕР, СИСТЕМА

					КІК.КР.Б – 123 – 16 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект локальної комп'ютерної мережі будівельної компанії	Літ.	Арк.	Аркушів
Розроб.		Литвинюк В.С.		10.06				
Керівник		Петрося Р. В.		2008			4	102
Реценз.		Граф М. С.		2008				
Н. контр.		Петрося Р.		2008				
Затверд.		Єфіменко І.А.		18.06			ФІКТ, Гр. КІ-4	

ANNOTATION

Diploma project contains 102 pages of text, 26 figures, 4 tables of references to 12 references.

The aim of the work is to design a local computer network of a construction company and to develop recommendations for optimizing information security processes for it.

The result of the qualification work is the development of a local computer network of the construction company.

Keywords: INFORMATION PROTECTION, INFORMATION SECURITY, SWITCH, ROUTER, NETWORK ARCHITECTURE, OBJECT OF PROTECTION, ORGANIZATION OF PROTECTION, POLYNOCYTICS AND POLYNOCYTICS.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	8
ВСТУП.....	9
РОЗДІЛ 1 ДОСЛІДЖЕННЯ ПИТАННЯ НЕОБХІДНОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ	11
1.1 Загальна характеристика компанії «GoodBud»	11
1.2 Аналіз технічної архітектури компанії.....	12
1.3 Аналіз програмної архітектури та даних компанії.....	14
1.4 Аналіз оброблюваних у компанії даних компанії	19
1.5 Класифікація основних загроз на підприємстві	22
1.6 Статистичний аналіз появи інцидентів кібербезпеки та росту виконуваних кібератак	27
1.7 Висновки до розділу 1	33
РОЗДІЛ 2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМПАНІЇ.....	35
2.1 Нормативно-правова база регулювання заходів забезпечення інформаційної безпеки підприємства	35
2.2 Методики побудови комплексної системи захисту інформації.....	36
2.3 Висновки до розділу 2	43
РОЗДІЛ 3 ПРОЕКТУВАННЯ РОЗМІЩЕННЯ ВУЗЛІВ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ	44
3.1 Обґрунтування мережевої архітектури та адресації хостів	44
3.2 Підбір необхідного активного та пасивного мережевого обладнання	48

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

3.3	Налаштування серверного сегменту комп'ютерної мережі.....	50
3.4	Налаштування доступу до ресурсів та технології захисту	54
3.5	Реалізація моделі комп'ютерної мережі за допомогою Packet Tracer .	58
3.6	Класифікація методів захисту інформації у комп'ютерних системах	61
3.7	Організаційно-правовий захист інформації.....	67
3.8	Інженерно-технічний захист інформації	70
3.9	Фізичні методи та засоби захисту інформації.	71
3.10	Апаратні методи та засоби захисту інформації.....	72
3.11	Програмні методи та засоби захисту інформації.....	73
3.12	Криптографічні методи та засоби захисту інформації	76
3.13	Об'єкти захисту	79
3.14	Планування та реалізація систем захисту	82
3.15	Методи захисту інформації	84
3.16	Розробка захисту для основних активів компанії.....	87
3.17	Висновки до розділу 3	96
ВИСНОВКИ		98
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ		100
ДОДАТКИ.....		103

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CHAP - Challenge Handshake Protocol

CPT - Cisco Packet Tracer

EAP - Extensible Authentication Protocol

PAP - Password Authentication Protocol

PPP - Point-to-Point Protocol

SSH - Secure Shell Protocol

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

ІТЗ - інженерно-технічний захист

КСЗІ - комплексна система захисту інформації

ОС – операційна система

ПЗ – програмне забезпечення

СКУД - система контролю і управління доступом

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність дослідження. Предметом захисту в будь-якій інформаційній системі підприємства є інформація. Основними особливостями інформації є те, що вона не матеріальна, її параметри неможливо виміряти фізичними методами і приладами, і те, що інформація зберігається і передається за допомогою матеріальних носіїв. Людина здатна отримати інформацію тільки тоді, коли вона записана на один з матеріальних носіїв: мозок людини, машинні носії, паперовий носій, електромагнітні і звукові хвилі і інші носії інформації.

Інформація має перелік властивостей. З точки зору інформаційної безпеки найбільш значущими є конфіденційність, доступність, цілісність. Так само важливою властивістю є цінність, важливість для власника інформації.

Основна інформація, всіх рівнів конфіденційності, в сучасних організаціях, на підприємствах збирається, зберігається, обробляється і передається в комп'ютерних системах. Все менше число організацій в даний час використовує централізовані системи, зараз найбільш затребувані розподілені комп'ютерні системи.

Зазначені комп'ютерні системи включають в себе велику кількість різних інформаційних систем і програмних продуктів. Кожен компонент може мати в собі вразливість, яка є загрозою для безпеки комп'ютерної системи в цілому. Передача інформації в розподілених системах відбувається по каналам зв'язку, часто не належить організації, за якими злоумисник може отримати доступ до ресурсів організації.

Для запобігання втрат пов'язаних з витоком інформації, несанкціонованих і ненавмисних дій в організаціях проводять діяльність із захисту інформації. Ця діяльність ґрунтується на програмі інформаційної безпеки організації та побудови ефективних центрів забезпечення інформаційної та кібербезпеки. Дана робота описує вимоги і принципи систем захисту інформації. Система захисту включає в себе правові норми, технічні, програмні та криптографічні

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

засоби, методи і механізми забезпечення інформаційної безпеки. Вся діяльність щодо забезпечення безпеки спрямовані на одночасне забезпечення критеріїв конфіденційності, цілісності та доступності.

Актуальність проблеми, яка розглядається в рамках роботи, обумовлена необхідністю захисту інформації та створення ефективних центрів забезпечення інформаційної та кібербезпеки будівельної компанії, розробкою інженерних і організаційних заходів з протидії можливим загрозам і порушникам.

Об'єктом дослідження є захист інфраструктури локальної мережі компанії.

Предмет дослідження – використання різноманітних систем та методів захисту інформації в компанії.

Для вирішення поставленого завдання необхідно:

- здійснити аналіз компанії "GoodBud" з метою забезпечення для неї інформаційної безпеки;
- розробити проектування локальної комп'ютерної мережі будівельної компанії;
- розробити рекомендації для оптимізації процесів забезпечення інформаційної безпеки компанії.

Методи дослідження – опрацювання літератури за даною темою, дослідження питання необхідності забезпечення інформаційної безпеки компанії, розглядання основних методів забезпечення захисту від загроз інформаційної безпеки у компанії, вивчення методики побудови комплексної системи захисту інформації.

Практичне значення одержаних результатів: розробка проекту локальної комп'ютерної мережі будівельної компанії із застосуванням комплексної системи захисту інформації від несанкціонованого доступу.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ПИТАННЯ НЕОБХІДНОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

1.1 Загальна характеристика компанії «GoodBud»

Компанія «GoodBud» пропонує весь комплекс загальнобудівельних робіт – від створення проектної документації до виконання чистових оздоблювальних робіт та комплектації об'єктів матеріалами за оптовими цінами. Діяльність фірми сконцентрована на повному забезпеченні процесу будівництва саун, бань, басейнів, турецьких бань тощо. від вибору проекту та закінчуючи здаванням реалізованого будівельного об'єкту «під ключ». Поєднання найкоротших термінів виконання замовлень та прийнятних цін, застосування сучасних матеріалів та дотримання високої якості роблять компанію «GoodBud» досить конкурентоспроможною у сфері будівництва.

Будівельна компанія «GoodBud» має значний досвід у монтажі та проведенні робіт з влаштування інженерних систем та обладнання, використовує у роботі сучасні передові технології та обладнання. Робочі бригади, що займаються монтажем, мають високу кваліфікацію та солідний досвід, які дозволяють виконувати замовлення у найкоротші терміни без зайвих затримок, а також прокласти інженерні системи у місцях, до яких досить складно забезпечити нормальний доступ. Досвідчені співробітники фірми проводять якісні консультації з монтажу, заміни або модернізації інженерних мереж, а також розповідають про нові тенденції у розвитку інженерних систем, про найбільш оптимальні, якісні та економічні рішення завдань, які необхідно реалізувати.

Будівельна компанія «GoodBud», що займається роботами з влаштування інженерних систем та обладнання, забезпечує комплексний підхід до виконання поставлених цілей, починаючи від дослідження та аналізу об'єктів, збору даних та проведення необхідних вимірів, складання проектно-кошторисної документації та закінчуючи пристроєм, монтажем та експлуатаційним тестування інженерних систем.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

У таблиці 1.1 наведено загальні технічні характеристики компанії.

Таблиця 1.1 - Характеристика компанії

<i>№ n/n</i>	<i>Найменування характеристики (показника)</i>	<i>Значення показника на певну дату</i>	<i>Одиниці виміру</i>
1	Річний оборот	80562000	грн.
2	Балансова вартість підприємства	46586000	грн.
3	Річний фонд заробітної плати	37000000	грн.
4	Кількість працівників	24	чол.
5	Кількість партнерів підприємства	60	шт.
6	Рентабельність підприємства	не менше 16%	

1.2 Аналіз технічної архітектури компанії

Головний офіс знаходиться на 12-му поверсі двадцятиповерхової офісної будівлі, у правому крилі. Офіс розташований у діловій частині міста. З трьох сторін оточений різними спорудами, четверта сторона виходить на автомобільну дорогу. Із сходу, на відстані 20 метрів, розташована висотна офісна будівля з паркувальним майданчиком. З північної сторони, на відстані 20 метрів, розташована багатоповерхова житлова будівля. З південної сторони, на відстані 20 метрів, розташована адміністративна будівля. З західної сторони розташована автомобільна дорога.

Приміщеннями, що підлягають особому захисту, є кабінет керівника та приміщення для проведення конфіденційних переговорів. Об'єкт обладнаний приміщеннями для конфіденційних переговорів. Підприємство працює 7 днів на

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

тиждень. Графік роботи з 9:00 до 19:00, з перервою на обід з 12:00 до 13:00. У період обідньої перерви організація не займається основною діяльністю, служба охорони та, зокрема, співробітник бюро пропусків відповідно до інструкції з охорони та пропускового режиму обідають на місці.

Компанія «GoodBud» складається з таких структурних підрозділів:

- Служба інформаційної безпеки – служба, яка виконує функції допоміжних процесів організації, вона виконує функції з інформаційної безпеки організації, пропускового режиму, організації фізичної охорони активів. Служба інформаційної безпеки розташована у службовому приміщенні (див. рис. 1.1);
- Юридичний відділ – відділ основних бізнес-процесів компанії, він займається роботою зі справами клієнтів, організовує діяльність представників компанії в судах та досліджує різні зміни у законодавстві.. Юридичний відділ знаходиться у службовому приміщенні (див. рис. 1.1);
- Бухгалтерія - служба, що займається веденням бухгалтерської та податкової звітності, що за сумісництвом виконує функції фінансового відділу, тим самим, розподіляючи фінансові потоки внутрішнього та зовнішнього середовища організації, у тому числі, бухгалтерія фінансує діяльність служби безпеки підприємства;
- Служба охорони –відповідає за організацію та ведення пропускового режиму у компанію та здійснює охоронну діяльність. Вона розташовується в окремому приміщенні (див. рис.11);
- Клієнтський відділ – відділ, який організовує взаємодію компанії з клієнтами. У клієнтському відділі укладаються бізнес-контракти компанії, надаються звіти про виконану роботу клієнтам;
- Відділ кадрів – виконує функції із забезпечення вакансій у компанії, управлінню людськими ресурсами, ведення особових справ працівників;
- Серверна - сховище основних баз даних та іншу інформацію з грифом «суворо конфіденційно». Доступ до неї тільки у працівників відділу безпеки.

Структурний склад компанії показаний на рис. 1.1

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

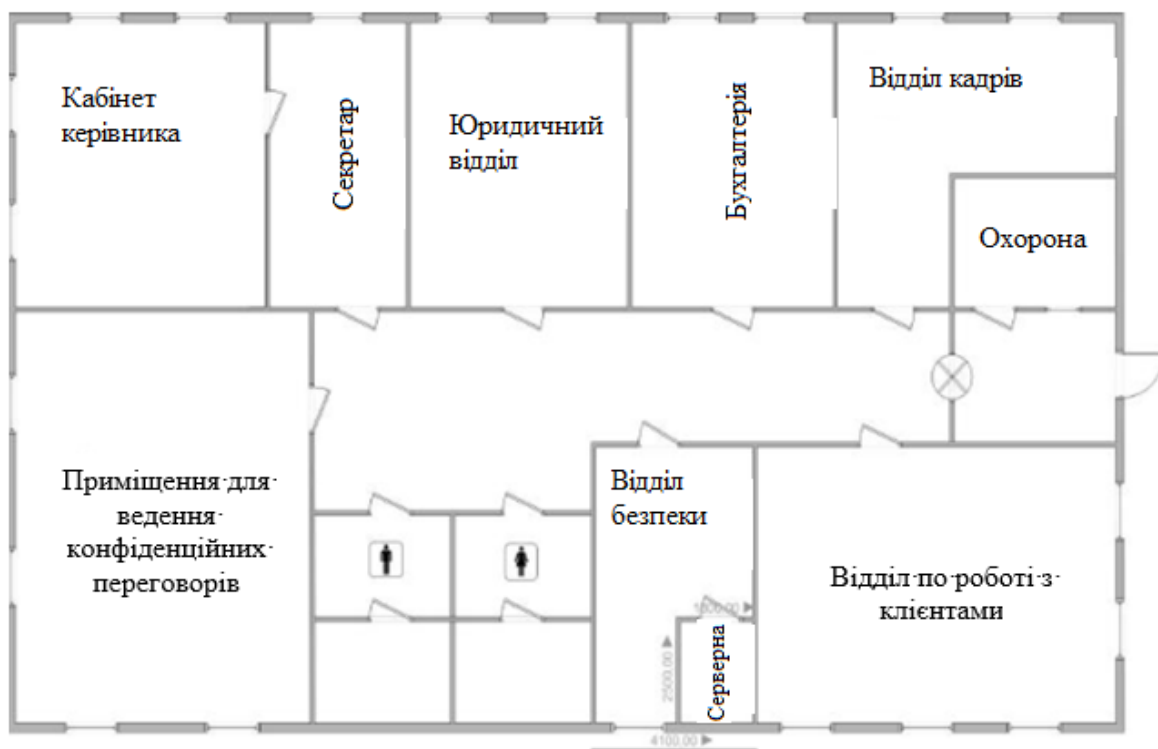


Рисунок 1.1 – Структурний склад компанії

1.3 Аналіз програмної архітектури та даних компанії

Склад внутрішніх документів із забезпечення ІБ можна поділити на чотири групи у вигляді ієрархічної структури (див. рис. 1.2):

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.2 – Структура внутрішньої документації щодо забезпечення ІБ в організації

1. Документи, що містять положення корпоративної політики ІБ організації (документи першого рівня), визначають високорівневі цілі, зміст та основні напрямки діяльності із забезпечення ІБ, призначені для організації загалом.

До таких документів має належати:

- концепція інформаційної безпеки;
- політика інформаційної безпеки;
- межі дії системи забезпечення інформаційної безпеки (включаючи перелік відомостей про конфіденційний характер);
- модель порушника та загроз інформаційної безпеки.

2. Документи, що містять положення приватних політик (документи другого рівня), деталізують положення корпоративної політики ІБ стосовно однієї або кількох областей ІБ, видів та технологій діяльності організації. До таких документів належать:

- положення про комерційну таємницю;
- політика управління ризиками;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

- політика корпоративної мережі;
- політика системи контролю та управління доступом тощо.

3. Документи, що містять положення ІБ, що застосовуються до процедур, а саме до порядку виконання дій або операцій забезпечення ІБ (документи третього рівня). Такі документи містять правила і параметри, що встановлюють спосіб здійснення та виконання конкретних дій, пов'язаних з ІБ, в рамках технологічних процесів, що використовуються в організації, або обмеження щодо виконання окремих дій, пов'язаних з реалізацією захисних заходів, у технологічних процесах, що використовуються (технічні завдання, регламенти, порядки, інструкції);

4. Документи, що містять свідчення виконаної діяльності щодо забезпечення ІБ (документи четвертого рівня), відображають досягнуті результати (проміжні та остаточні), що стосуються забезпечення ІБ організації.

У даній роботі безліч документів та актів, які безпосередньо стосуються інформаційної безпеки буде агреговано, а частина не буде розглянута докладно. Як об'єкт для розробки будуть використовуватись документи першого, другого та третього рівня, а саме:

- Перелік відомостей про конфіденційний характер (1 рівень);
- Політика інформаційної безпеки (1 рівень);
- Приватна модель загроз інформаційній безпеці (1 рівень);
- Положення про комерційну таємницю (2 рівень);
- Інструкція з організації охорони та пропускового режиму (3 рівень).

Відповідно до ДСТУ ISO 27001-2006 для забезпечення впевненості в тому, що інформація захищена на належному рівні її необхідно класифікувати виходячи з правових вимог, її конфіденційності, а також цінності та критичності для організації. Відповідно до прийнятої в організації системи класифікації повинна бути розроблена та реалізована сукупність процедур маркування та обробки інформації.[2]

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

В компанії «GoodBud» інформація класифікується за вимогами СТР-К НСТЕК, що мають для цієї організації рекомендаційний характер. Основними класифікаційними ознаками є:

1. Належність інформації до підрозділу організації;
2. Зміст інформації у певних базах даних або на певних паперових носіях;
3. За ступенем та природою конфіденційності;
4. По співробітникам, які мають доступ до інформації;
5. По організаціях або фізичних осіб, які мають доступ до конфіденційної інформації, але не працюють у компанії «GoodBud».

Таким чином, для кожного відділу організації можна виділити інформацію, з якої він працює:

- бухгалтерія - відділ, який виконує функції фінансового обліку та аудиту, ведення бухгалтерської та податкової звітності, а також всі функції з фінансування та управління фінансами організації. У бухгалтерії містяться відомості про бухгалтерський баланс, податкові та бухгалтерські звітності, відомості про фінансовий стан організації, її рахунки;
- відділ по роботі з клієнтами - містить усі відомості, отримані від клієнтів організації, відомості про переговори та наради, що проводяться, а також, тактичні плани та моделі розвитку організації;
- юридичний відділ - ядро бізнес-процесів організації, оскільки організація займається колекторською діяльністю, юридичний відділ виконує більшу частину функцій із забезпечення основних процесів діяльності організації, займається стратегічним та тактичним плануванням, бере участь у всіх важливих для підприємства подіях. Для даного відділу доступна вся інформація за винятком бухгалтерської звітності та інформації про реалізацію СЗІБ;
- відділ кадрів – містить лише відомості про співробітників організації, основна функція відділу – управління людськими ресурсами в організації;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

- служба безпеки - зважаючи на свою діяльність допущена практично до всіх відомостей в організації, за деяким незначним винятком. Служба безпеки в компанії «GoodBud», крім своєї основної діяльності, включає службу охорони та системного адміністратора організації, що виконує за сумісництвом функції адміністратора інформаційної безпеки. Начальник охорони допускається до відомостей про організацію охорони на підприємстві та до персональних даних, що дозволяють ідентифікувати співробітників та клієнтів організації. Системного адміністратора допущено до всіх відомостей електронних баз даних через свою діяльність з їх налаштування та захисту;
- генеральний директор та його заступники мають допуск до всієї конфіденційної інформації, оскільки є засновниками ТОВ «GoodBud».

Для визначення зв'язку класів інформаційних активів, допущених осіб, внутрішнього грифу конфіденційності та баз даних, у яких містяться активи. Таким чином, за допомогою переліку відомостей конфіденційного характеру можна визначити який співробітник допущений до певного типу інформації, який гриф має ця інформація і в якій базі даних вона знаходиться. Відповідно до ДСТУ 27001-2006, перелік інформаційних активів, які підлягають захисту, є частиною корпоративної політики інформаційної безпеки, тобто. стратегічним документом першого рівня (див. рис. 1.2).

У компанії «GoodBud» обробляється дуже багато персональних даних, як клієнтів, і співробітників організації, всього 50 000 суб'єктів ПД. Для виконання вимог НСТЕК, та спрощення побудови системи захисту ІСПДн, доступ до ПД у переліку відомостей конфіденційного характеру розбито на 3 групи:

1. Доступ до персональних даних 3 та 4 категорії співробітників організації;
2. Доступ до персональних даних 3 та 4 категорії клієнтів організації;
3. Доступ до персональних даних усіх категорій, будь-яких суб'єктів.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Такий поділ дозволяє обмежити доступ до персональних даних 2 категорії співробітників служб допоміжних процесів, таких як служба охорони, служба відділу кадрів тощо.

Маркування інформації за типами необхідне дотримання вимог стандарту ДСТУ 27001.[2]

В компанії «GoodBud» вся інформація, що захищається поділяється на два рівні конфіденційності:

1. Конфіденційно - до такої інформації належить вся інформація, що захищається, яка не має гриф строго конфіденційно;
2. Суворо конфіденційно - така інформація включає:
 - персональні дані клієнтів та співробітників організації 2 категорії;
 - відомості про концепцію розвитку підприємства, стратегічні плани розвитку, функціональні, маркетингові, фінансові та логістичні моделі ведення бізнесу;
 - тактичні плани розвитку, інформація про поточні та планові контракти;
 - відомості, що розкривають систему, засоби захисту інформації, порядок обробки та передачі інформаційних активів.

1.4 Аналіз оброблюваних у компанії даних компанії

В даній підтемі можна розглянути основні моменти, які пристосовані для обробки даних компанії, іншою, зазвичай ІТ-компанією з залученням максимального захисту для всіх оброблюваних типів даних. Нижче приведена низка опціональних застосунків, які напряду, чи опосередковано забезпечують безпечну обробку будь-яких даних.

Дублювання інформації є одним із найефективніших способів забезпечення цілісності інформації.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Під надійністю розуміється властивість системи виконувати покладені на неї функції за певних умов обслуговування та експлуатації. Надійність КС на будь-якому підприємстві досягається на етапах розробки, виробництва, експлуатації. Важливим напрямом у забезпеченні надійності КС є своєчасне виявлення та локалізація можливих несправностей у роботі її технічних засобів. Значно скоротити можливості внесення суб'єктивних помилок розробників дозволяють сучасні технології програмування.

Блокування помилкових операцій. Помилкові операції в роботі КС можуть бути викликані не лише випадковими відмовами технічних та програмних засобів, а й помилками користувачів та обслуговуючого персоналу. Для блокування помилкових дій використовуються технічні та апаратно-програмні засоби, такі як блокувальні тумблери, запобіжники, засоби блокування запису на магнітні диски та інші.

Оптимізація. Одним з основних напрямків захисту є скорочення кількості помилок користувачів і персоналу, а також мінімізація наслідків цих помилок. Для досягнення цих цілей необхідні: наукова організація праці, виховання та навчання користувачів та персоналу, аналіз та вдосконалення процесів взаємодії людини та КС.

Мінімізація збитків. Запобігти стихійним лихам людина поки що не в змозі, але зменшити наслідки таких явищ у багатьох випадках вдається. Мінімізація наслідків аварій та стихійних лих для об'єктів КС може бути досягнута шляхом: правильного вибору місця розташування об'єкта (подалі від місць, де можливі стихійні лиха); обліку можливих аварій та стихійних лих при розробці та експлуатації КС; організації своєчасного оповіщення про можливі аварії; навчання персоналу боротьби зі стихійними лихами та аваріями, методами ліквідації їх наслідків.

Основним способом захисту від зловмисників вважається використання про засобів ААА, чи ЗА (аутентифікація, авторизація, адміністрування).

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Авторизація (санкціонування, дозвіл) – процедура, за якою користувач при вході в систему опізнається та отримує права доступу, дозволені системним адміністратором, до обчислювальних ресурсів (комп'ютерів, дисків, папок, периферійних пристроїв) [8].

Авторизація виконується програмою і включає ідентифікацію та аутентифікацію.

Ідентифікація – надання ідентифікатора, яким може бути несекретне ім'я, слово, число, реєстрації користувача в КС. Суб'єкт вказує ім'я користувача, що пред'явлений ідентифікатор порівнюється з переліком ідентифікаторів. Користувач, у якого ідентифікатор зареєстровано у системі, розцінюється як правомочний (легальний). Синонімом ідентифікатора є логін – набір літер та цифр, унікальний для даної системи.

Аутентифікація – автентифікація, тобто те, що пред'явлений ідентифікатор дійсно належить суб'єкту доступу. Виконується на основі зіставлення імені користувача та пароля. Після автентифікації суб'єкту дозволяється доступом до ресурсів системи з урахуванням дозволених йому повноважень.

Найчастіше застосовуваними методами авторизації є методи, засновані на використанні паролів (секретних послідовностей символів). Пароль можна встановити на запуск програми, окремі дії на комп'ютері або мережі. Крім паролів для підтвердження справжності можуть використовуватися пластикові картки та смарт-картки.

Адміністрація – це реєстрація дій користувача в мережі, включаючи спроби доступу до ресурсів. Для своєчасного припинення несанкціонованих дій, контролю за дотриманням встановлених правил доступу необхідно забезпечити регулярний збір, фіксацію та видачу за запитами відомостей про всі звернення до захисту.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

1.5 Класифікація основних загроз на підприємстві

До сутнісних проявів загрози відносяться:

1. Джерело деструктивного впливу на інформацію (від кого чи чого виходять ці впливу);
2. Види деструктивного впливу на інформацію (як);
3. Методи деструктивного впливу на інформацію (якими прийомами, діями здійснюються і реалізуються види деструктивного впливу).

Основні типи загроз інформаційній безпеці:

- Загрози конфіденційності – несанкціонований доступ до даних (наприклад, отримання сторонніми особами про стан рахунків клієнтів).
- Загрози цілісності – несанкціонована модифікація, доповнення чи знищення даних (наприклад, внесення змін до бухгалтерських проводок з метою розкрадання коштів).
- Загрози доступності – обмеження або блокування доступу до даних (наприклад, неможливість підключитися до сервера з базою даних у результаті DDoS-атаки).
- Загрози достовірності – це властивість інформації, що виражається у суворій приналежності суб'єкту, що є її джерелом, або суб'єкту, від якого ця інформація прийнята.[1]

В першу чергу для забезпечення ефективного захисту інформації, розглядають та аналізують всі фактори, що становлять загрозу інформаційній безпеці.

Стихійні лиха та аварії загрожують найбільш руйнівними наслідками для КС, оскільки останні зазнають фізичного руйнування, інформація втрачається, або доступ до неї стає неможливим.

Збої та відмови складних систем неминучі. В результаті збоїв та відмов порушується працездатність технічних засобів, знищуються та спотворюються дані та програми, порушується алгоритм роботи пристроїв.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Умисні загрози пов'язані з цілеспрямованими діями порушника.

Основними ненавмисними штучними загрозами є:

- ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування обладнання, видалення, спотворення файлів з важливою інформацією або програм, у тому числі системних тощо);
- неправомірне включення обладнання або зміна режимів роботи пристроїв та програм;
- ненавмисна, псування носіїв інформації;
- запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання чи зациклювання) чи незворотні зміни у системі;
- нелегальне використання та використання неврахованих програм (ігрових, навчальних, технологічних та інших., які є необхідні виконання порушником своїх службових обов'язків) з наступним необґрунтованим витрачанням ресурсів (завантаження процесорів, захоплення оперативної пам'яті та пам'яті на зовнішніх носіях);
- зараження комп'ютера вірусами;
- необережні дії, що призводять до розголошення конфіденційної інформації або роблять її загальнодоступною;
- розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо);
- проектування архітектури системи, технології обробки даних, розробка прикладних програм з можливостями, що становлять загрозу для працездатності системи та безпеки інформації;
- ігнорування організаційних обмежень (встановлених правил) при ранзі у системі;
- вхід до системи в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв тощо);

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

- некомпетентне використання, налаштування чи неправомірне відключення засобів захисту персоналом служби безпеки;
- пересилання даних за помилковою адресою абонента (пристрою);
- введення помилкових даних;
- ненавмисне ушкодження каналів зв'язку.

Основні навмисні штучні загрози характеризуються можливими шляхами умисної дезорганізації роботи, виведення системи з ладу, проникнення в систему та несанкціонованого доступу до інформації:

- фізична руйнація системи (шляхом вибуху, підпалу тощо) або виведення з ладу всіх або окремих найважливіших компонентів комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу тощо);
- від виключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);
- дії щодо дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи тощо);
- застосування підслуховуючих пристроїв, дистанційна фото- та відеозйомка тощо;
- перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку, а також наведення активних випромінювань на допоміжні технічні засоби, які безпосередньо не беруть участі в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);
- перехоплення даних, що передаються каналами зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження у зв'язок та авторизації користувача та подальших спроб їх імітації для проникнення в систему;
- розкрадання носіїв інформації (дисків, мікросхем пам'яті, що запам'ятовують пристроїв та персональних ЕОМ);

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

- несанкціоноване копіювання носіїв інформації;
- розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації тощо);
- читання залишків інформації з оперативної пам'яті та із зовнішніх запам'ятовуючих пристроїв;
- незаконне отримання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, імітації інтерфейсу системи тощо) з подальшим маскуванням під зареєстрованого користувача («маскарад»);
- несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку, апаратний блок кодування тощо;
- незаконне підключення до ліній зв'язку з метою роботи «між рядків», з використанням пауз у діях законного користувача від його імені з подальшим введенням хибних повідомлень або модифікацією повідомлень, що передаються;
- незаконне підключення до ліній зв'язку з метою прямої заміни законного користувача шляхом його фізичного відключення після входу в систему та успішної автентифікації з подальшим введенням дезінформації та нав'язуванням хибних повідомлень.[1]

Велику загрозу безпеці інформації в КС є несанкціонована модифікація алгоритмічної, програмної та технічної структур системи, яка отримала назву «закладка». Як правило, «закладки» впроваджуються у спеціалізовані системи та використовуються або для безпосереднього шкідницького впливу на КС, або для забезпечення неконтрольованого входу до системи.

Одним з основних джерел загроз є використання спеціальних програм, що отримали загальну назву «шкідливі програми». До таких програм належать:

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

– вірус – це штучна комп'ютерна програма або частина коду, який викликає несподівані, як правило, негативні наслідки, виконані програмним шляхом на вашому комп'ютері. Віруси часто маскуються під ігри або зображення з відомими брендами або назвами;

– «хробаки» - програми, які виконуються щоразу при завантаженні системи, що мають здатність переміщатися в КС або мережі та самовідтворювати копії. Лавиноподібне розмноження програм призводить до перевантаження каналів зв'язку, пам'яті, а потім блокування системи;

– «троянські коні», Trojan - шкідлива програма, яка претендує на доброякісний додаток; програма-троян цілеспрямовано робить те, що користувач зовсім не чекає або не хоче робити. Трояни не є вірусами, тому що вони не розмножуються, але ці програми можуть бути настільки ж руйнівними як і віруси. Багато людей використовують НЕ ПРАВИЛЬНИЙ термін для позначення троянів чи вірусів;

– СПАМ (S.P.A.M. – у перекладі з англ. «обрізки, шматки, залишки») є небажаним отримання будь-яких електронних повідомлень. Існує СПАМ в електронній пошті, на сайтах, у банерах, у новинах, СПАМ веб-пошуку, СПАП у блогах, та мобільний спам за SMS. СПАМ це реклама, що вводить в оману користувача.

Крім всього зазначеного вище, дуже великий ризик для будь-якої компанії несуть програми-шпигуни, які мають широкий спектр діяльності, переважно це небажані програми, які використовують заражені комп'ютери для отримання комерційної вигоди. Вони можуть доставити небажані спливаючі вікна з рекламою, вкрасти особисту інформацію (включаючи фінансову інформацію, таку як номери кредитних карток), контролювати веб-сторінки для діяльності в маркетингових цілях, або ваш колишній шлях запиту на авторизовані сайти з вашими даними.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Окрім зазначених вище загроз безпеки, існує також загроза витоку інформації, яка з кожним роком стає дедалі значущою проблемою безпеки. Щоб ефективно справлятися з витоками, необхідно знати, яким чином вони відбуваються.

Не можна обійти і той факт, що нині активно розвивається фішинг – технологія Інтернет-шахрайства, яка полягає у крадіжці особистих конфіденційних даних, таких як паролі доступу, номери кредитних карток, банківських рахунків та іншої персональної інформації. Фішинг (від англ. Fishing - риболовля) розшифровується як вивузування пароля. В основному використовується метод проведення масових розсилок від імені популярних компаній або організацій, що містять посилання на помилкові сайти, які зовні не відрізняються від справжніх.

Незалежно від специфіки конкретних видів загроз, інформаційна безпека має зберігати цілісність, конфіденційність, доступність.

Ще одним видом загроз інформаційній безпеці є загроза розкриття параметрів КС. В результаті її реалізації не завдається жодної шкоди інформації, що обробляється в КС, але при цьому істотно посилюються можливості прояву первинних загроз.[17]

1.6 Статистичний аналіз появи інцидентів кібербезпеки та росту виконуваних кібератак

Систему захисту на підприємстві можна як безперервне протидія власника активів і порушника, який намагається рахунок створення загроз інформаційної безпеки, з допомогою на вразливості активів створити ризик безпеки активів

Власник для протидії порушнику вживає контрзаходи щодо зменшення ризику за рахунок впливу на вразливість (див. рис. 1.3). Таке уявлення системи захисту дозволяє будувати моделі інформаційної безпеки з урахуванням теорії ігор. У такому разі учасниками будуть відповідно власник активів та порушник, а як матриця сценаріїв для кожного учасника будуть використані можливі дії над

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

елементами (загрози, вразливості, активи, ризики, контрзаходи). Таким чином, буде матрична, некорпоративна гра з ненульовою сумою: виграшем для зловмисника буде кількісна величина завданих збитків, а для власника – величина втраченого виграшу зловмисника, в оптимальному вирішенні гри – збереження повної вартості активів та запобігання збиткам.

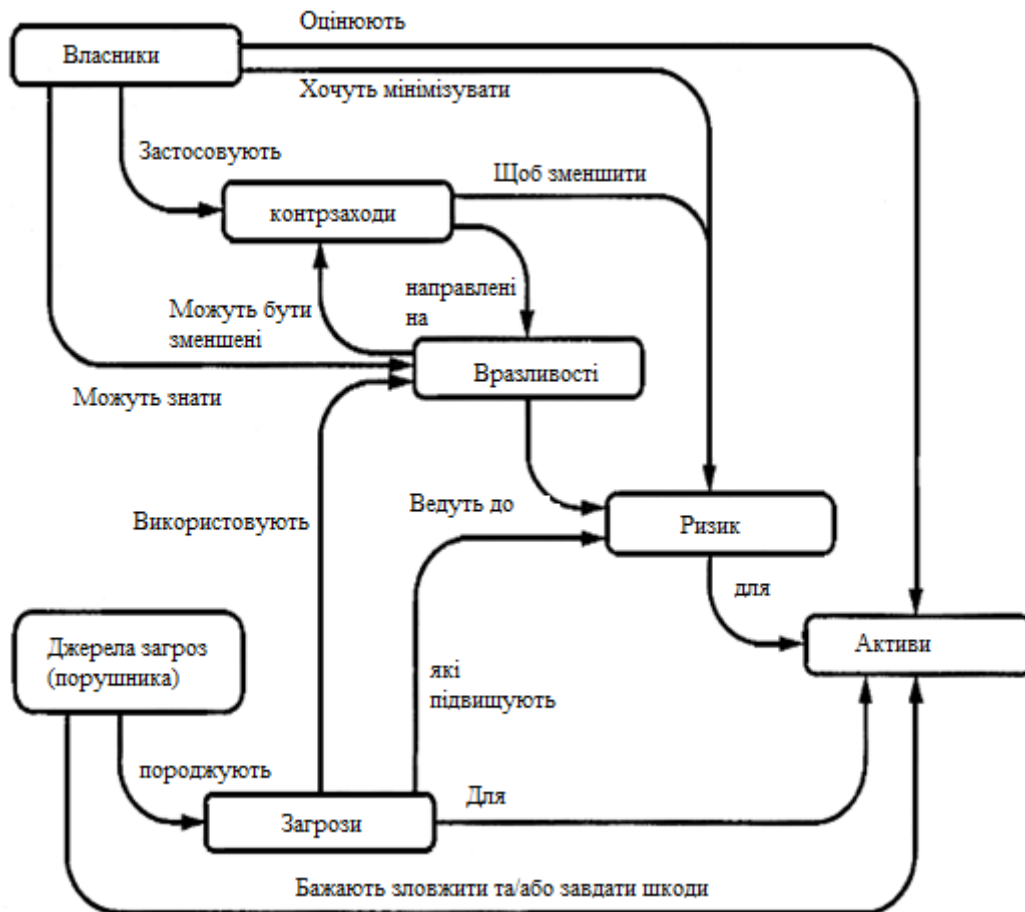


Рисунок 1.3 – Процесний підхід до захисту інформації

Таким чином, виходячи з процесного підходу до захисту інформації, діяльність із захисту має будуватися на послідовному вирішенні наступних завдань:

1. Ідентифікація активів;
2. Ідентифікації та побудови моделі порушника;
3. Ідентифікація та побудова моделі загроз інформаційній безпеці;
4. Ідентифікація вразливостей активів та системи захисту;

5. Оцінка комплексного показника можливості заподіяння шкоди власнику активів - ризику;

6. Прийняття рішення щодо захисту інформації від наявних ризиків інформаційної безпеки.

Комплекс заходів щодо планування, організації, координації та контролю виконання зазначених завдань, документування процесів, регламентування дій процесу захисту - є організаційною складовою захисту інформації.

Технічна складова - сутність самих контрзаходів у технічному вигляді, це може бути спеціальне обладнання та засоби захисту, засоби безпосередньої фізичної охорони активів тощо.

Можна розглянути систему інформаційної безпеки ТОВ «GoodBud» відповідно до процесного підходу до захисту інформації. Вирішення проблеми з ідентифікації активів наведено в даній роботі, результатом такої оцінки є документально оформлений перелік відомостей конфіденційного характеру.

Ідентифікація порушника – комплексне завдання організаційного та технічного захисту інформації, таке завдання вирішується при створенні всього комплексу документів із захисту інформації, всіх рівнів. Побудова моделі порушника - складне та багатоаспектне стратегічне завдання вищої ланки служби інформаційної безпеки. У рамках даної роботи необхідно обмежуватися тим, що в компанії «GoodBud» така модель існує і відмінно виконує свої функції, як документ вищого рівня поруч із політикою інформаційної безпеки.

Мета цього опису – побудова моделі загроз ІБ (інформаційної безпеки). Оскільки компанія «GoodBud» невеликого розміру, але містить величезну кількість персональних даних та комерційної таємниці, модель загроз об'єднуватиме у собі вразливості організації, загрози ІБ та ризики ІБ як результативний комплексний показник. Оцінка ризиків проводитиметься експертними методами, включаючи метод багатовимірної шкалювання. За основу для побудови моделі загроз використано рекомендації ISO 27005, ISO 13335-3.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Приватна модель загроз включає п'ять блоків, на основі яких виконується оцінка ризиків та висновки про їх актуальність, зафіксований у додатках до приватної моделі загроз:

1. Основні вразливості, оцінені експертами як актуальні для компанії «GoodBud», дозволяють ідентифікувати загрози безпеці (див. рис. 6). Перелік вразливостей активів є відправною точкою для діяльності комісії з аналізу ризиків. Зміна такого переліку у приватній моделі загроз у компанії «GoodBud» не рекомендується;

2. Рівні інформаційної інфраструктури дозволяють оцінити рівень загрози ІБ з точки зору розподілу інформаційних потоків. Ідентифікація таких рівнів у моделі загроз дозволяє спрямовувати використовувати діяльність із захисту від конкретних загроз до конкретних підрозділів. Наприклад, загроза на фізичному рівні, швидше за все, буде адресована підрозділу, який займається фізичною охороною активів;

3. Джерела загроз ІБ - основа для побудови моделі порушника, що дозволяє ідентифікувати джерело загрози при побудові системи захисту від конкретних загроз. Експерти використовують цей показник для складання переліку актуальних загроз;

4. Критерії оцінки безпеки інформаційних активів такі критерії у приватній моделі загроз компанії «GoodBud» встановлено з повним дотриманням Законодавства України.

5. Метод оцінки ризиків загроз ІБ – у приватній моделі загроз компанії «GoodBud» описано методику обробки та оцінки ризиків, Основою служить експертні методи. Ризик складається з двох показників:

✓ Імовірність реалізації загрози – визначається експертами на основі статистичних даних, власного досвіду та досвіду інших організацій. Експертна комісія у кількості 5 осіб надає кожній загрозі показник від 1 до 1000, значення якого збігається з частками від ймовірності реалізації загрози.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

✓ Збиток від реалізації загрози – визначається таким самим чином, як і ймовірність, експерти привласнюють залежно від своїх припущень оцінку щодо кожної загрози. 1 бал відповідає збитку одну тисячу гривень.

На основі цих двох показників розраховується міра ризику, що дорівнює їхньому результуючому фактору. Таким чином, за допомогою цього показника можна дати оцінку важливості загрози та будувати методику оцінки ефективності системи захисту.

Виходячи з діяльності організації, її особливостей, моделі порушника, переліку відомостей конфіденційного характеру та політики інформаційної безпеки були зроблені такі дії для створення приватної моделі загроз:

✓ Було створено експертну комісію з аналізу наявної системи захисту інформації в організації, і на підставі цього було сформульовано перелік вразливостей інформаційних активів за допомогою послідовно застосованого методу мозкового штурму та методу багатокритеріальної оцінки;

✓ За допомогою тієї ж експертної комісії було оформлено попередній перелік загроз ІБ.

На підставі наявних уразливостей активів та поточної системи безпеки, експертною комісією з кожної загрози ІБ була проведена оцінка імовірнісної складової оцінки ризику та оцінка можливої шкоди від реалізації такої загрози. Загальна схема діяльності За результатами оцінки ризиків щодо кожної загрози ІБ можуть бути прийняті такі типи рішень:

✓ Збереження ризику - тим загрозам, ймовірність реалізації яких мізерна, або збитки від якої вважається прийнятним. Критерії для відсіву таких ризиків визначаються завдання на обробку ризиків. Загрози з таким ризиком не представлені у приватній моделі загроз та відсіяні на етапі обробки ризиків.

✓ Зниження ризику - дії, спрямовані на: виправлення, усунення, запобігання, мінімізацію впливу, стримування, виявлення, відновлення, контроль та розуміння ризику. У випадку діяльності зі зниження ризику показано малюнку

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

7. Перелік загроз, ризик реалізації яких вимагає зниження, є основною частиною моделі загроз. Вимоги щодо зниження рівня ризику визначаються на підставі моделі загроз приватними політиками інформаційної безпеки та іншою документацією.

✓ Запобігання ризику - Якщо ідентифіковані ризики вважаються надто високими або вартість здійснення інших варіантів обробки ризику перевищує вигоду, може бути прийняте рішення, щоб уникнути ризику повністю, виходячи із запланованої або існуючої діяльності, сукупності видів діяльності або змінюючи умови, за яких керують діяльністю. Наприклад, викликані природні ризики можуть бути ефективніше вирішені у вартісному еквіваленті порівняно з альтернативою, якщо фізично перемістити засоби обробки інформації в місце, де ризик не існує або знаходиться під контролем. У разі ТОВ «GoodBud» використовує методи запобігання ризику шляхом регламентації видів діяльності організації у статуті, наприклад, організація не займається питаннями, пов'язаними з державною таємницею та обробкою персональних даних 1 категорії;

✓ Перенесення ризику - Перенесення ризику стосується рішення розділити певні ризики із зовнішніми сторонами. Перенесення ризику може створити нові або змінити існуючі ідентифіковані ризики. Тому може бути необхідною додаткова обробка ризику. Перенесення може бути зроблене страхуванням, яке підтримує наслідки або, укладаючи субпідрядний договір на партнера, роль якого повинна контролювати інформаційну систему та вжити безпосередніх дій, щоб зупинити атаку, перш ніж вона зробить певний рівень ушкоджень. Діяльність полягає у прийомі ризиків сторонніх організацій, зниженні їх та отриманні на цьому прибутку. Що стосується ризиків ІБ, організація використовує страхування обладнання, включаючи сервери та СВТ.

✓ Після описаної вище оцінки ризиків, експерти з ІБ склали приватну модель загроз, що включають як загрози комерційній таємниці, так і загрози персональним даним. Для виконання вимог НСТЕК оцінка ризиків здійснення загроз ПД була проведена за допомогою методики НСТЕК, а приватна модель загроз була розроблена на основі базової моделі загроз НСТЕК.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

✓ Після складання приватної моделі загроз вживаються організаційні та технічні заходи щодо протидії загрозам ІБ. У ТОВ «GoodBud» такі заходи описуються у приватних політиках безпеки, положеннях про КТ та ПД, вимоги до процедур ІБ, посадові інструкції та записи з ІБ.

1.7 Висновки до розділу 1

Опис основних концептів ІС у компанії «GoodBud» системи інформаційної безпеки (СІБ) виявиться ефективною, якщо вона надійно підтримуватиме виконання правил політики безпеки. Етапи побудови політики безпеки – це внесення до опису об'єкта автоматизації структури цінності та проведення аналізу ризику, а також визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають певний рівень цінності.

Правові заходи забезпечення безпеки комерційної таємниці є першочерговими, т. я. вони мають забезпечити ефективне функціонування інших заходів забезпечення конфіденційності інформації. З цього погляду правові заходи є первинними стосовно інших заходів.

Усі документи мають пройти погодження з юридичною службою підприємства, затверджено керівництвом та введено в дію наказом по підприємству. При цьому необхідно також враховувати, що документи повинні відповідати законам та іншим правовим документам України.

За результатами аналізу об'єкта захисту та огляду технічних засобів можна розробити проект модернізації існуючої інформаційної системи. Модернізована система забезпечує надійний захист об'єкта від несанкціонованого проникнення та повністю відповідає вимогам компанії у сфері ІТ-безпеки. При виборі технічних засобів особлива увага приділялася їх функціональним характеристикам та технічній сумісності пристроїв. Представлений концепт-модель системи повні-

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

стю відповідає вимогам для компанії «GoodBud» та готовий бути одним з основних компонентів найбільш стабільної та безпечної обробки інформації в процесі роботи компанії.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМПАНІЇ

2.1 Нормативно-правова база регулювання заходів забезпечення інформаційної безпеки підприємства

Правова форма захисту інформації – це захист інформації, який «... базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів в галузі інформатики, інформаційних відносин та захисту інформації. Вона регламентує права і обов'язки суб'єктів інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації».

Правовий захист інформації загальновизнаний на міжнародному (міжнародні договори, угоди, конвенції, декларації тощо) та державному рівні. На державному рівні правовий захист регулюється державними та відомчими нормативно-правовими актами.[8]

Розроблена на їх основі система законодавчих актів та нормативних, організаційних та адміністративних документів повинна забезпечити організацію ефективного контролю за їх виконанням правоохоронними органами та реалізацію засобів захисту та відповідальності суб'єктів інформаційних відносин. Цю систему можна віднести до морально-етичних норм поведінки, які склалися традиційно або розвиваються з поширенням обчислювальних засобів у суспільстві.

Законодавчі документи щодо захисту інформації в Україні:

- Закон України «Про інформацію»;
- Закон України «Про державну таємницю»;
- Закон України «Про захист персональних даних»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про електронний цифровий підпис»;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

- Закон України «Про Національну програму інформатизації»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Положення про порядок здійснення криптографічного захисту інформації в Україні;
- Стаття 31 Конституції України;

Державну політику у сфері захисту інформації відповідно до закону реалізує Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку України).

2.2 Методики побудови комплексної системи захисту інформації

Для визначення актуальних загроз для підприємства необхідно знати показник вихідної захищеності.

Під рівнем вихідної захищеності розуміється узагальнений показник, що залежить від технічних і експлуатаційних характеристик (Y1) [15].

В таблиці 2.1 представимо розрахунок показників вихідної захищеності підприємства.

Таблиця 2.1 – Показники вихідної захищеності

Технічні та експлуатаційні характеристики	Рівень захищеності		
	високий	середній	низький
За територіальною розгалуженістю:			
Локальна мережа, розгорнута в межах близько розташованих будівель	-	+	-
За наявністю з'єднання з мережами загального користування:			

Мережа, що має одноточковий вихід в мережу загального користування	-	+	-
<i>За вбудованими операціями із записами баз персональних даних:</i>			
Модифікація, передача	-	-	+
<i>Щодо розмежування доступу до персональних даних:</i>			
Доступ мають певні співробітники організації	-	+	-
<i>За наявністю з'єднань з іншими базами:</i>			
Використовується одна база, що належить організації	+	-	-
<i>За рівнем узагальнення (знеособлення):</i>			
Є інформація, що дозволяє ідентифікувати суб'єкта	-	-	+
<i>За обсягом даних, які надаються стороннім користувачам без попередньої обробки:</i>			
Система, що надає частину даних	-	+	-

Виходячи з даних, отриманих в таблиці 2.1, всього 14% показників- високого рівня захищеності, 57% - середнього рівня захищеності, 28,6% - низького рівня захищеності.

Отже, система має середній рівень захищеності. Для середнього рівня захищеності, характерний числовий коефіцієнт -5 [15].

Для визначення можливих каналів витоку інформації, виявлених на етапі обстеження, необхідно розробити документ «Приватна модель загроз безпеки конфіденційної інформації (КІ) при їх обробці для систем».

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Цей документ містить перелік загроз безпеки ІС, розрахунок актуальності яких розраховувався виходячи з рівня вихідної захищеності, уразливості, що дозволяють здійснити їх практичну реалізацію, а також методи і способи захисту інформації, що дозволяють знизити актуальність загроз до прийнятного рівня.

Загрози безпеці інформації, оброблюваної в ІС, що містяться в моделі загроз, можуть доповнюватися в міру виявлення нових джерел загроз в ІС.

Модель загроз складається на основі проведеного аналізу імовірнісних загроз інформаційної безпеки.

Приватна модель загроз представлена у вигляді таблиці 2.2.

Таблиця 2.2 – Модель загроз інформаційної системи

<i>Загрози</i>	<i>Існуючі заходи захисту</i>	<i>Вразливості</i>	<i>Імовірність реалізації</i>
1.1 Фізичний доступ порушника	Встановлена охоронна сигналізація і елементи фортифікації	—	Низька
1.2. Розголошення конфіденційної інформації, що зберігається на серверах	Трудовий кодекс України, трудовий договір.	Людський фактор (Шантаж, підкуп, погрози, помста, необережність)	Середня
1.3. Руйнування конфіденційної інформації на серверах за допомогою спеціальних програм і вірусів	—	Людський фактор (Шантаж, підкуп, погрози, помста, необережність), а також застарілий антивірусний захист	Середня

1.4.Копіювання конфіденційної інформації з сервера	Розмежування прав доступу користувачів	Користувачі не дотримуються заходів щодо інформаційної безпеки	Середня
1.5.Доступ з мереж загального користування до серверів	Функціонує міжмережевий екран, провайдер забезпечує додатковий захист	Міжмережевий екран із застарілим програмним забезпеченням, застарілий антивірусний захист	Середня
2.1.Фізичний доступ порушника до АРМ, копіювання конфіденційної інформації	Встановлено елементи фортифікації, встановлена охоронна сигналізація, розмежування прав доступу користувачів	Користувачі не дотримуються заходів щодо інформаційної безпеки	Середня
2.2.Розголошення конфіденційної інформації, що зберігається на АРМ	Трудовий кодекс, трудовий договір	Людський фактор (шантаж, підкуп, погрози, помста, необережність)	Середня
2.4.Доступ з мереж загального користування до АРМ	Функціонує міжмережевий екран, провайдер забезпечує додаткову захист	Міжмережевий екран із застарілим програмним забезпеченням, застарілий антивірусний захист	Середня
3.1.Фізичний доступ порушника до документів, електронних носіїв	Встановлено елементи фортифікації, встановлена	Користувачі не дотримуються заходів з інформаційної безпеки	Середня

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

	охоронна сигналізація.		
3.2.Розголошення конфіденційної інформації, що зберігається на документах, електронних носіях, винос документів за межі контрольованої зони	Трудовий кодекс трудоий договір	Людський фактор (шантаж, підкуп, погрози, помста, необережність)	Середня
3.3.Несанкціоноване копіювання, друк і розмноження конфіденційних документів	Встановлено елементи фортифікації, встановлена охоронна сигналізація	Користувачі не дотримуються заходів по ІБ	Середня

Після складання приватної моделі загроз для ІС були виявлені можливі загрози, ймовірність яких вище, ніж низька. Для розробки політики безпеки вважаємо, що дані загрози є актуальними [16].

При побудові даної моделі в першу чергу всіх порушників можна розділити на дві основні групи - це зовнішні і внутрішні.

Під зовнішніми порушниками для ІС варто розуміти в першу чергу конкуруючі організації, а також потенційні кримінальні та терористичні угруповання, а також потенційні корупційні елементи, що знаходяться в органах влади [17,18].

Найчастіше діяльність даних порушників спрямована в першу чергу на будь-які пасивні носії КІ, а також на копіювання, псування або знищення її носіїв.

Також дії зовнішніх порушників можуть бути спрямовані на персонал, і можуть проявлятися у вигляді різних загроз або підкупу, з метою отримання необхідної інформації, яка становить комерційну таємну.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Також дії зовнішніх порушників можуть бути направлені на переманювання співробітників компанії.

Але найбільшу загрозу можуть представляти собою внутрішні порушники, так як вони мають доступ до інформації, який має статус КІ, або, наприклад, знати про існуючі способи захисту даної інформації.

Таким чином, внутрішніми порушниками можуть бути як нечисті на руку керівники організації, рядові співробітники, а також шахраї або аферисти.

Крім цього, варто звернути увагу на те, що співробітники мають високий рівень самооцінки і можуть бути незадоволені або рівнем заробітної плати, або відносинами з керівництвом компанії або рядовими співробітниками.

Таким чином, в таблиці 2.3 модель порушника можна представити таким чином:

Таблиця 2.3 – Модель порушника

<i>Порушник</i>	<i>Мотив дії</i>	<i>Потенційні можливості</i>
Керівник	власна вигода	Мають доступ до обладнання на якому зберігається \ обробляється конфіденційна інформація. Мають права доступу до обладнання
Системний адміністратор, адміністратор безпеки	Образа, користь, помста, примус сторонньою організацією	Мають доступ до обладнання на якому зберігається \ обробляється конфіденційна інформація. Не мають прав доступу до обладнання
Співробітник		У деяких випадках мають доступ до обладнання на якому зберігається \ обробляється конфіденційна інформація.
Підрядник		

Колишній співробітник	Образ, користь, помста, примус сторонньою організацією	Мають доступ до обладнання на якому зберігається \ обробляється конфіденційна інформація з моменту звільнення до моменту закриття доступу до даних адміністратором. При звільненні адміністратора, особа зобов'язана проконтролювати позбавлення адміністраторських прав у звільненого адміністратора
Терористичні, екстремістські угруповання	Власна вигода, помста, примус	Примус (залякування, підкуп) співробітників, здійснення хакерських атак (при наявності виходу в мережу)
Кримінальні структури		
Конкуруючі організації		
Спеціальні служби іноземних держав		
Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів		Здійснення хакерських атак (при наявності виходу в мережу інтернет)

Відповідно до базової моделі загроз безпеки персональних даних, зовнішніми порушниками є: зовнішні суб'єкти, що здійснюють доступ до інформації, з використанням спеціальних програмних впливів за допомогою програмних вірусів, шкідливих програм, алгоритмічних або програмних закладок.

Відповідно з базовою моделлю загроз безпеки персональних даних, внутрішніми порушниками є:

– 1 категорія: співробітники адміністративно-господарського відділу (співробітники, що відповідають за електробезпеку, за пожежну безпеку, охорона, прибиральники), які мають доступ до технічних засобів, але не мають доступ до ПД;

– 2 категорія: начальники, керівники, фахівці відділів, які мають доступ до ресурсів з робочого місця;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

- 3 категорія: співробітники відомчих організацій, що мають віддалений доступ до ПД;
- 4-6 категорії: співробітники групи автоматизації, які мають повноваження адміністратора;
- 7 категорія: програмісти - розробники, що забезпечують супрвід;
- 8 категорія: програмісти - розробники, особи, які забезпечують поставку, супровід і ремонт.

Внутрішніх порушників категорії 4-6 можна виключити з потенційних, так як при розгляді кандидатур на дані посади проводиться додатковий аналіз відповідності вимогам і надійності.

Внутрішній порушник з категорії 7 і категорії 8 також виключаються з потенційних порушників, так як організації-постачальники здійснюють поставку обладнання або ТЗ на підставі договору, що вже тягне за собою фінансові ризики.

Отже, актуальними внутрішніми порушниками залишаються порушники категорій 1,2,3 і зовнішній порушник.

2.3 Висновки до розділу 2

Отже, перед розробкою рекомендацій для оптимізації процесів забезпечення інформаційної безпеки компанії, необхідно чітко знати всі компоненти та методики побудови комплексної системи захисту інформації, від яких буде залежати надійність захисту компанії. Безумовно, основою системи захисту інформації в компанії мають бути організаційні (адміністративні) заходи, стержнем яких є розробка та реалізація плану захисту. Але організаційні заходи без повсюдної підтримки їх фізичними та технічними (програмними та апаратними) засобами будуть слабкі. Тому при виборі засобів захисту необхідно звертати увагу не тільки на їхню надійність, але й на те, як вони підтримуватимуть розроблені організаційні заходи.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 3 ПРОЕКТУВАННЯ РОЗМІЩЕННЯ ВУЗЛІВ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

3.1 Обґрунтування мережевої архітектури та адресації хостів

Обладнання та програмне забезпечення:

1. Програмне забезпечення: Симулятор мережі GNS3, Virtual Box.
2. Операційні системи: Windows 10, Windows Server 2019
3. Апаратне забезпечення: маршрутизатор Cisco 2901-HSEC+/K9, комутатор Cisco WS-C2960-24TT-L, точка доступу MikroTik RBCAPGI-5ACD2ND

У комп'ютерній мережі використовуватиметься динамічно задані ір – адреси та маршрутизація буде динамічна.

Наша система містить 4 сегменти та 54 комп'ютери.

Наступний крок налаштування маршрутизатора:

- interface Ethernet1/0;
- ip address 192.168.10.2 255.255.0.0;
- no shutdown;
- interface Ethernet1/1;
- ip address 192.168.10.129 255.255.0.0;
- no shutdown.

Список інтерфейсів роутера показано на рис.3.1.

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Ethernet1/0	192.168.10.2	YES	manual	up	up
Ethernet1/1	192.168.10.129	YES	manual	up	up
Ethernet1/2	unassigned	YES	unset	administratively down	down
Ethernet1/3	unassigned	YES	unset	administratively down	down

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.1 – Список інтерфейсів роутера

Наступний крок налаштування маршрутизатора:

- interface Ethernet1/0;
- ip address 192.168.10.1 255.255.0.0;
- no shutdown;
- interface Ethernet1/1;
- ip address 192.168.10.65 255.255.0.0;
- no shutdown.

Список інтерфейсів маршрутизатора показано на рис. 3.2.

FastEthernet0/0	unassigned	YES unset	administratively down	down
FastEthernet0/1	unassigned	YES unset	administratively down	down
Ethernet1/0	192.168.10.1	YES manual	up	up
Ethernet1/1	192.168.10.66	YES manual	up	up
Ethernet1/2	unassigned	YES unset	administratively down	down
Ethernet1/3	unassigned	YES unset	administratively down	down

Рисунок 3.2 – Список інтерфейсів роутера

Для налаштування сервера для роботи як DNS і DHCP-сервера необхідно перейти у відповідні розділи та увімкнути дані служби. На рисунках 3.3 та 3.4 показані налаштування DNS і DHCP-сервера відповідно.

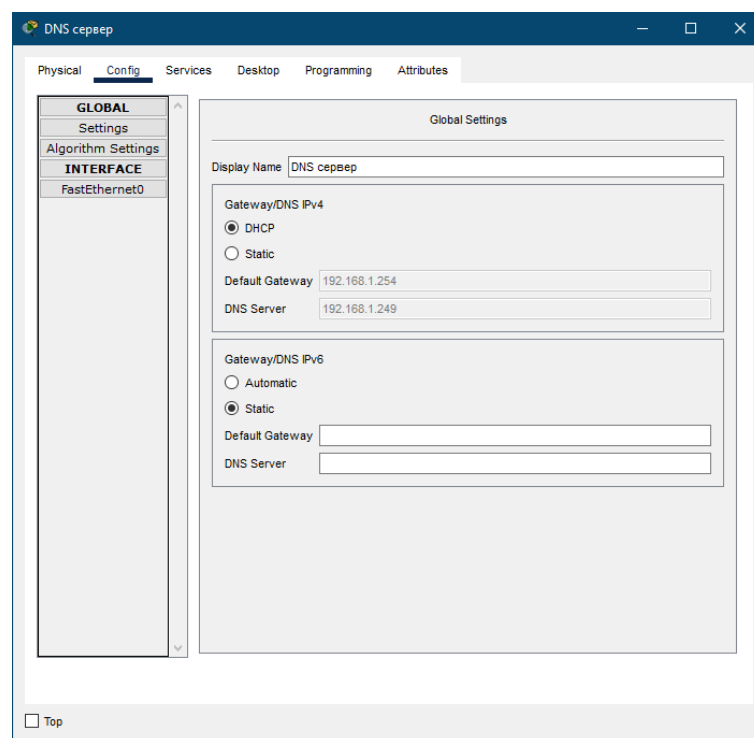


Рисунок 3.3 – Налаштування DNS сервера

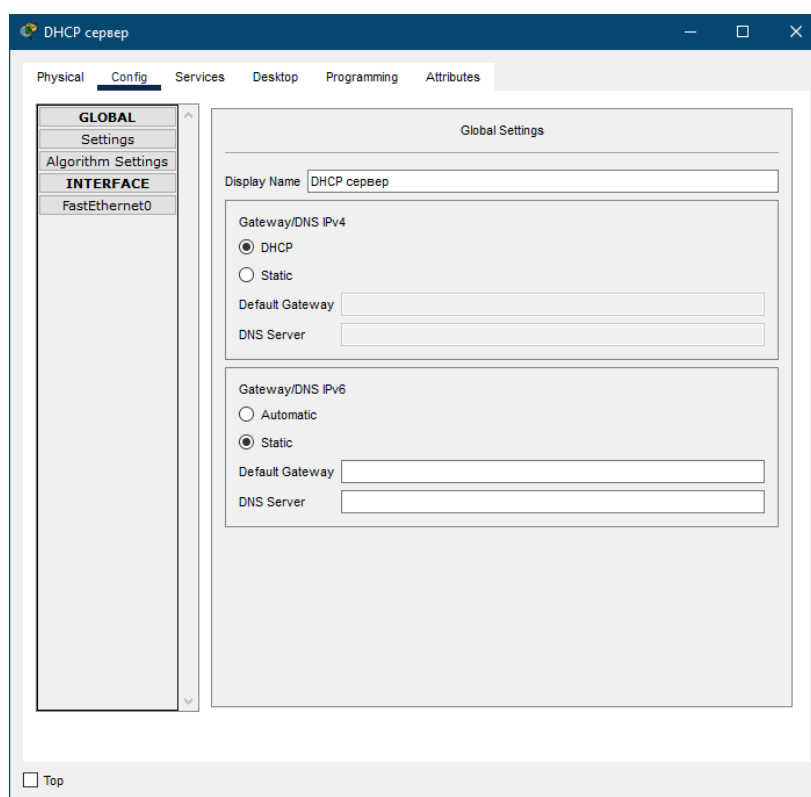


Рисунок 3.4 – Налаштування DHCP сервера

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Всі персональні комп'ютери локальної мережі підприємства мають динамічні IP адреси (рис. 3.5).

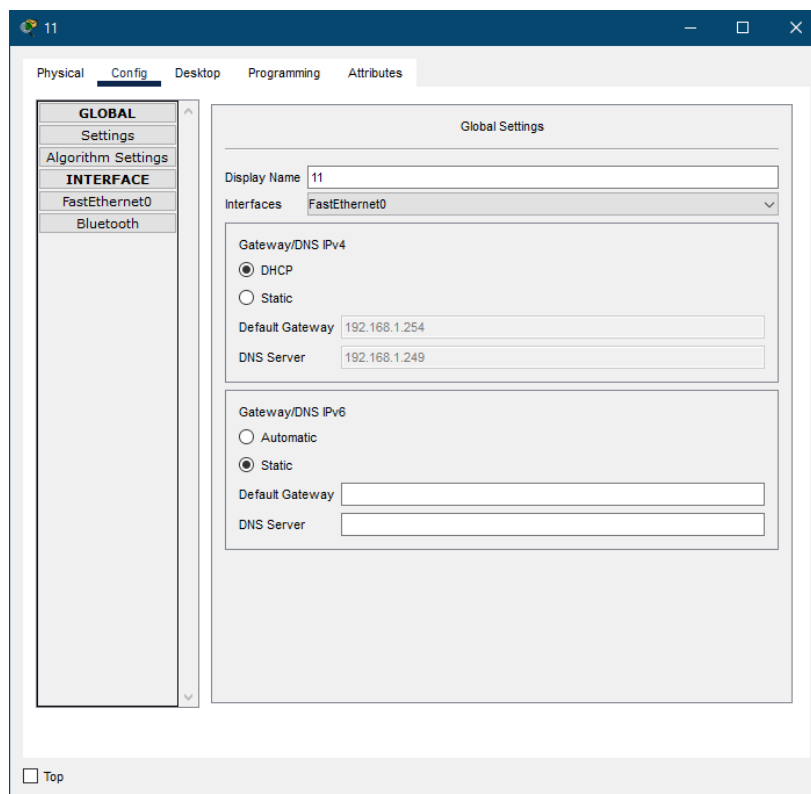


Рисунок 3.5 – Налаштування мережі для персонального комп'ютера

Всі ноутбуки підприємства під'єднані до локальної мережі за допомогою безпроводної мережі та використовують динамічну IP адресу (рис 3.6).

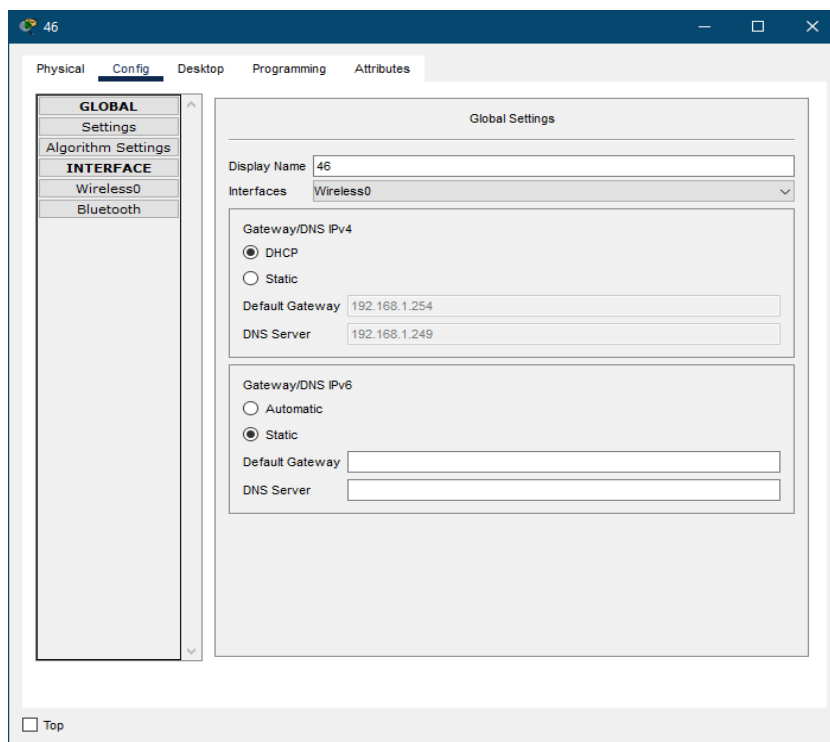


Рисунок 3.6 – Налаштування мережі для ноутбука

Для взаємодії із зовнішніми мережами ця мережа може бути підключена до мережі Інтернет. Для цього можна, наприклад, підключити один з роутерів до кручений пари провайдера. Для доступу до мережі Інтернет необхідно внести в таблиці маршрутизації роутерів зміни, що передбачають можливість передачі пакетів до мережі Інтернет. А також змінити відповідні налаштування на комп'ютерах (у нашому випадку, потрібно також внести зміни до налаштувань серверів).

3.2 Підбір необхідного активного та пасивного мережевого обладнання

У цьому підрозділі наведено список технічних пристроїв, які будуть використовуватись у розробленій мережі.

Для організації роботи мережі підприємства було використано 24-ох портовий комутатор Cisco Catalyst 2960-X та маршрутизатор Cisco 881 C881GW+7-A-K9.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Cisco Catalyst 2960-X – лінійка комутаторів, що стекуються з підтримкою технології доступу Gigabit Ethernet. Моделі Cisco Catalyst 2960-X забезпечують комутацію другого рівня (L2 layer) та оснащені одним основним блоком живлення з можливістю встановлення додаткового, резервного джерела живлення. Дані комутатори забезпечені 24 або 48 портами Gigabit Ethernet, підтримують технології Power over Ethernet/Power over Ethernet Plus (PoE/PoE+) і чотири канали Gigabit Ethernet Small Form-Factor Pluggable (SFP) або два канали 10 Gigabit Ethernet Small Form-Factor (SFP+). Комутатори працюють на базі двох ядерних процесорів 600МГц. Технологія FlexStack-Plus дозволяє зібрати стек з 8 комутаторів та забезпечує пропускну здатність 80 Гбіт/сек. Для забезпечення візуалізації та контролю трафіку різних програм у мережі, Cisco додали функцію NetFlow Lite, яка дозволяє інженерам моніторити та керувати потоками даних на всіх сегментах мережі.

Ця платформа, прийшовши на зміну пристроям із серії Catalyst 2960-S, розроблена з метою скорочення операційних витрат та сукупної вартості володіння. Вона забезпечує захист інвестицій завдяки можливості змішаного стекування FlexStack+ з комутаторами Cisco Catalyst 2960-S та 2960-SF (у цьому випадку у стек можна поєднати до 4 комутаторів).

Використовуючи такі технології, як Cisco EnergyWise та Energy Efficient Ethernet, комутатори Catalyst 2960 серії X забезпечують найкращу у своєму класі енергоефективність, а механізм Switch Hibernation Mode дозволяє в окремих випадках досягти радикального скорочення енергоспоживання з економією електроенергії до 80%.

Програмне забезпечення (feature set) комутаторів Cisco Catalyst 2960-X випускається в образах LAN Base та Lan Lite Image. LAN Base має більш широкий функціонал, включаючи покращену безпеку (ACLs), DHCP Snooping та додаткові функції контролю доступу - Web authentication та розширення 802.1x, додаткові можливості установок якості обслуговування QoS, підтримка надлишкового живлення RPS та великої кількості SFP-портів. Функції Flex Links та Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host,

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, та IP SLA (responder) та інше. Образ LAN Lite підтримує базові функції Layer 2 і призначений переважно для використання в невеликих організаціях, а LAN Base повністю підтримує функції Layer 2 та розрахований на застосування у середніх та великих організаціях. Комутатори Cisco Catalyst 2960-XR випускаються із набором IP Lite. Набір функцій IP Lite підтримує вже Layer 3 (тобто має функції маршрутизації) і орієнтований на середні і великі організації..

Маршрутизатори *Cisco 881 C881GW+7-A-K9* використовуються на підприємствах, в компаніях, де необхідно організувати безвідмовну роботу мережі. Забезпечують широкомасштабний захист. Просте керування дозволяє легко налаштовувати пристрій, підтримувати високий рівень безпеки, виконувати необхідні функції.

Характеристики:

- Тип: роутер;
- WAN-порт: 1 FE;
- LAN-порти: 4-port 10/100-Mbps;
- Стандарт Wi-Fi: 802.11n/g;
- Вбудований комутатор: 4-port switch;
- Канальний протокол: Ethernet, Fast Ethernet.

3.3 Налаштування серверного сегменту комп'ютерної мережі

Для стабільної та надійної роботи мережі налаштуємо DHCP та DNS сервери.

DNS (система доменних імен) відповідає за відповідність доменних імен та IP-адрес. Доменне ім'я - це не тільки адреса в інтернеті, наприклад selectel.ru, але також ім'я комп'ютера в локальній мережі, наприклад Director PC. DNS про-

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

водить з'єднувальну лінію між IP та літерно-числовим доменним ім'ям комп'ютера або веб-сайту. DHCP займається виділенням та призначенням IP з області. Очевидно, що два протоколи мають тісно взаємодіяти між собою.

DHCP – це протокол динамічної конфігурації вузлів мережі. Служить для автоматичної видачі мережевих параметрів, таких як ір-адреса, мережна маска, адреси мережевих шлюзів і серверів DNS, комп'ютерам (хостам, вузлам) локальної мережі (ЛОМ), що знову підключаються.

У Windows Server всі основні служби поставляються у вигляді ролей - у спрощеному вигляді це завдання, які виконуватиме цей сервер, наприклад: DHCP-сервер, DNS-сервер, Доменні служби Active Directory, "Служби друку та документів та і т.д.

Для налаштування DHCP-сервер необхідно перейти в оснащення диспетчер сервера у вкладку DHCP і вибрати сервер "Диспетчер DHCP".

Виділивши потрібний сервер у лівому списку вибираємо протокол, який будемо налаштовувати - ipv4 або ipv6. Зупинимося на IPv4. Розгорнемо відповідне дерево та виберемо з контекстного меню “Створити область”. Областю називається діапазон виданих IP-адрес. Запуститься майстер створення області.

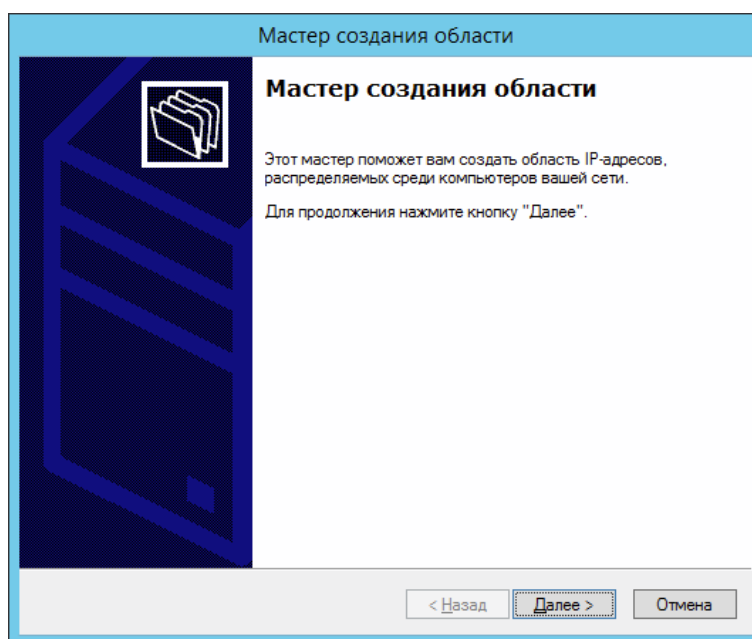


Рисунок 3.7 – Майстер створення області

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

На наступній сторінці потрібно встановити назву області.

Рисунок 3.8 – Встановлення назви області

На наступному кроці потрібно власне задати діапазон ір-адрес, які надаватиме цей сервер і маску підмережі в нотації CIDR (довжина) або числами.

Рисунок 3.9 – Створення діапазону ір-адрес

За необхідності можна задати ір-адреси, що виключаються з оренди - ці адреси видаватися хостам не будуть. Далі можна змінити термін оренди - чим

		Литвинюк В.С.			KIK.KP.B – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

більше тим більш довгий час ір-адреса закріплюється за вузлом мережі. за замовчуванням 8 днів.

Мастер создания области

Срок действия аренды адреса
Срок действия аренды определяет, как долго клиент может использовать IP-адрес из этой области.

Срок действия аренды адреса, как правило, должен быть равен среднему времени нахождения компьютера в одной и той же физической сети. Например, в сети, состоящей в основном из портативных компьютеров или клиентов коммутируемого подключения, рекомендуется устанавливать непродолжительный срок действия аренды адреса.

Для стабильной сети, состоящей в основном из настольных компьютеров на фиксированных рабочих местах, более приемлем длительный срок действия аренды адреса.

Установите срок действия аренды адресов области, выдаваемых этим сервером.

Не более:

дней: часов: минут:

< Назад Далее > Отмена

Рисунок 3.10 – Задання терміну оренди

Далі водимо IP-адреси маршрутизаторів і тиснемо додати (рис. 3.11).

Мастер создания области

Маршрутизатор (основной шлюз)
Вы можете указать маршрутизаторы или основные шлюзы, распределяемые этой областью.

Чтобы добавить IP-адрес маршрутизатора, используемого клиентами, введите его в поле ниже.

IP-адрес:

Добавить
Удалить
Вверх
Вниз

< Назад Далее > Отмена

Рисунок 3.11 – Налаштування IP-адреси маршрутизаторів

Завершуємо налаштування області..

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

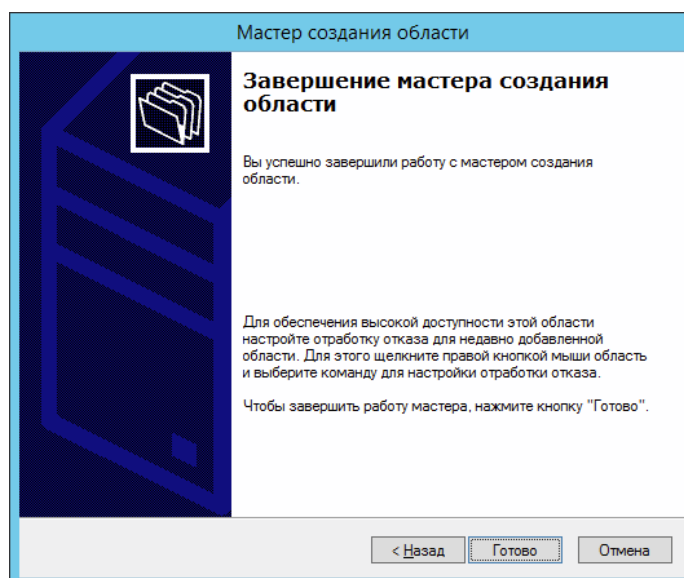


Рисунок 3.12 – Завершення налаштування DHCP-сервера

3.4 Налаштування доступу до ресурсів та технології захисту

Налаштування доступу до ресурсів підприємства були розроблені заходи безпеки інформації на програмному рівні.

Під розробкою заходів безпеки інформації на програмному рівні розуміються спеціальні програми, що включені в програмне забезпечення комп'ютера для виконання лише функцій безпеки.

До найважливіших заходів інформаційної безпеки програмного забезпечення належать:

- Програмне забезпечення для ідентифікації та автентифікації користувачів комп'ютера;
- Програми для розмежування доступу користувачів до ресурсів комп'ютера;
- Програми для шифрування інформації;

– Програмне забезпечення для захисту інформаційних ресурсів (системного та прикладного програмного забезпечення, баз даних, засобів комп'ютерного навчання тощо) від несанкціонованої зміни, використання та копіювання.

Слід розуміти, що з ідентифікацією з погляду комп'ютерної інформаційної безпеки розуміється унікальне розпізнавання унікального імені суб'єкта комп'ютера. Аутентифікація означає підтвердження того, що надане ім'я відповідає суб'єкту (підтвердження справжності суб'єкта).

Розробка заходів безпеки інформації на програмному рівні була здійснена в операційній системі Windows 10 за допомогою налаштувань такого інструменту, як антивірусу Avast.

Налаштування антивірусу Avast

Avast Antivirus Professional - антивірус, здатний виявити велику кількість відомих вірусів, а також невідому діяльність і віруси, що самодифікуються, для яких не можливе пряме виявлення.

Основні характеристики:

- Високий рівень виявлення вірусів, троянів та хробаків.
- Резидентний (в режимі реального часу) та звичайний сканер.
- Сканування архівів.
- Перевірка вхідної та вихідної електронної пошти.
- Глибока інтеграція у систему.
- Карантин ізольований від операційної системи, що забезпечує більшу безпеку роботи. Жоден файл, що зберігається в карантині, не може бути запущений.
- Мінімальне число хибних спрацьовувань
- Велика кількість налаштувань.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

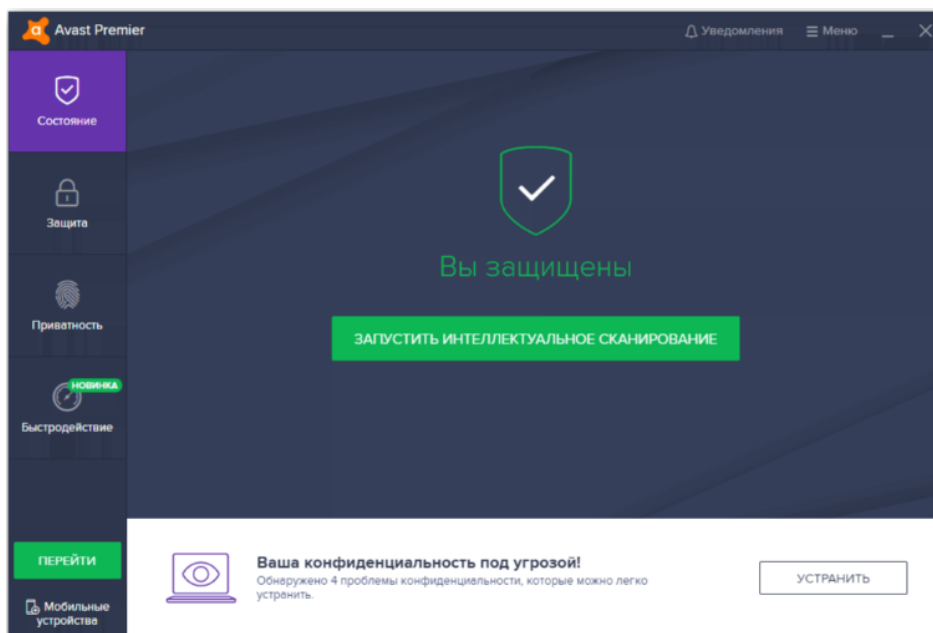


Рисунок 3.13 – Головне меню програми Avast Antivirus

Програма Avast Antivirus дозволяє вибрати необхідні області сканування - локальні диски, змінні носії або вибрані ні папки. Є можливість налаштування резидентного захисту: вимкнено, звичайний або високий рівень. Вибираємо високий рівень резидентного захисту.

Існує можливість вибору типу сканування: експрес-сканування, звичайне сканування, повне сканування.

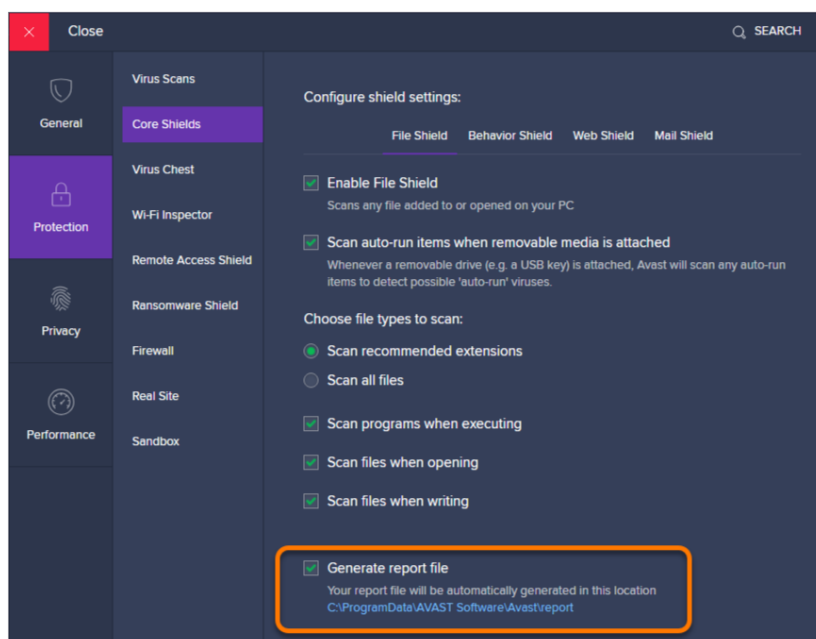


Рисунок 3.14 – Визначення типу сканування

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пєтросян Р.В.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

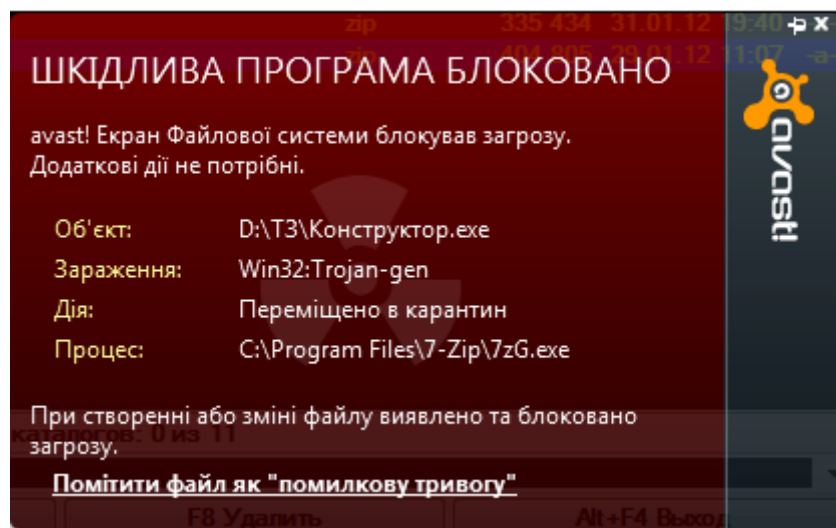


Рисунок 3.15 – Резидентний сканер видає повідомлення про виявлення троянів

Також програма дозволяє оновлювати антивірусні бази (часте оновлення антивірусної системи є обов'язковим), забезпечує автоматичне оновлення через Інтернет вірусних баз даних або навіть самого доданку.

До недоліків цієї програми можна віднести такі:

- ✓ При включенні резидентного захисту високого рівня та повного сканування продуктивність комп'ютера різко знижується;
- ✓ Необхідність оновлення антивірусних баз;
- ✓ Неможливість лікувати заражені файли: можливо або видалити заражені файли, або помістити їх у вірусне сховище.

Потужний резидентний модуль Avast здатний виявити вірус, перш ніж він заразить комп'ютер. Особливість нової версії програми – евристичний аналіз поштових повідомлень. Це дуже корисно для захисту від нових, невідомих вірусів та хробаків, яких не можна виявити звичайними засобами. Евристичний модуль ретельно вивчає кожне поштове повідомлення та спостерігає за підозрілими

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

ознаками, які могли б виявити присутність вірусу. Коли кількість цих ознак перевищує встановлений користувачем поріг, повідомлення вважають небезпечним, і користувач отримує попередження.

3.5 Реалізація моделі комп'ютерної мережі за допомогою Packet Tracer

Для опису процесів та параметрів налаштування маршрутизаторів компанії Cisco, було спроектовано модель мережі у програмі моделювання роботи мережі Cisco Packet Tracer, основне вікно якої наведено на рисунку 3.16.

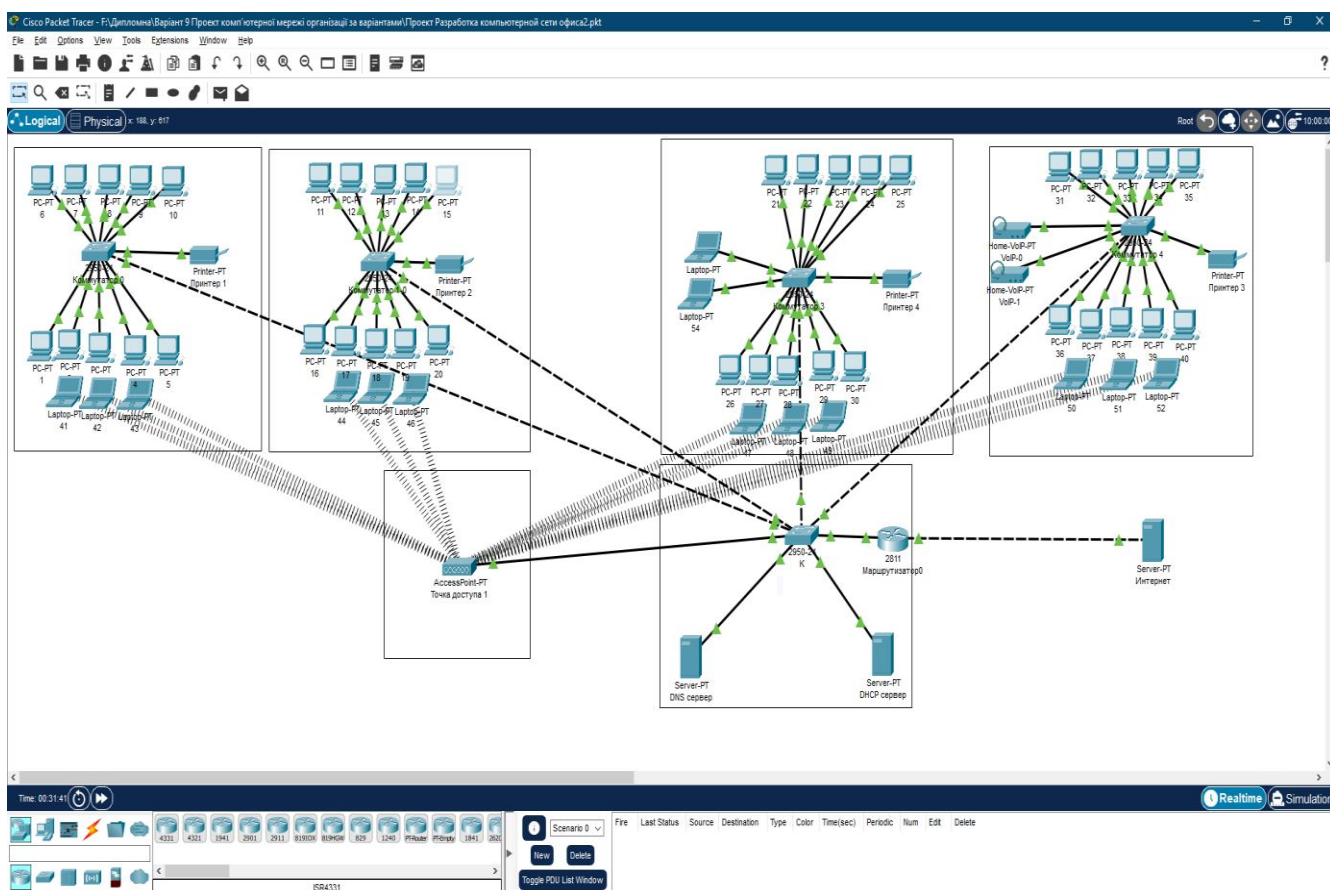


Рисунок 3.16 – Робоча область Cisco Packet Tracer

На рис. 3.16 представлена зібрана та модернізована у плані безпеки мережа. У ключових місцях системи передачі даних встановлені маршрутизатори Cisco.

		Литвинюк В.С.			KIK.KP.B – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

До параметрів конфігурації робочої станції відносяться параметри вказівки IP-адреси та маски підмережі, якщо не встановлено режим динамічного розподілу адрес. Параметри конфігурації робочої станції показані рисунку 3.17.

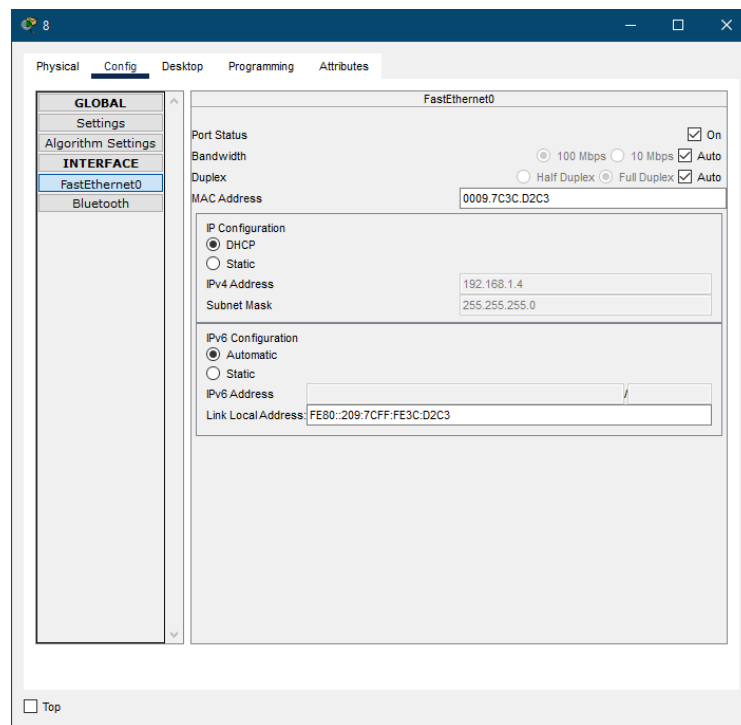


Рисунок 3.17 – Динамічне задання адресації

Процес налаштування комутаторів та портів комутаторів зводиться до налаштування віртуалізації мереж.

Налаштування можна проводити через розширений інтерфейс користувача, так і через командний рядок терміналу обслуговування системи IOS комутатора. На рис. 3.18 наведено приклад налаштування мережного з'єднання між комутатором і хостом, що входить до мережі обслуговування даного комутатора.

3.6 Класифікація методів захисту інформації у комп'ютерних системах

Всупереч поширеній думці звичайні факти власними силами, ні про що не говорять – вони набувають значення порівняно з іншими фактами. Якщо деякі відомості не несуть нам смислового навантаження або ж вони нові для нас, такий факт залишиться нам лише фактом. Щодня ми дізнаємося про масу нової інформації, потрібної і не дуже. Більшу частину ми, природно, дізнаємося з Інтернету. Дані та відомості про деякі об'єкти, що знаходяться у вільному доступі, належить усім без винятку. Крім того, в Інтернеті люди часто передають один одному величезну кількість особистої інформації. Тому наше суспільство часто називають «інформаційним», адже людство в буквальному розумінні почало залежати від інформації, якою вона володіє.

У світі інформація несе певну для людини цінність. Як і будь-яку іншу цінність, інформацію варто захищати від її неправомірного спотворення або несанкціонованого доступу до неї. Багато користувачів залишилися б незадоволеними, якби інформація особистого характеру, якою вони обмінюються в різних соціальних мережах, була б у загальному користуванні. Тому захист даних від несанкціонованого доступу є одним із пріоритетних завдань при проектуванні будь-якої інформаційної системи. Але як правильно захистити інформацію? І чи існує абсолютний захист інформації? Саме ці питання будуть розглянуті у роботі.

Черговий етап технологічної революції, що відбувається нині у світі, тягне за собою серйозні зміни в економіці, соціальній структурі суспільства. Масове застосування нових технологічних засобів, на основі яких здійснюється інформатизація, стирає геополітичні межі, змінює спосіб життя мільйонів людей. Разом про те, інформаційна сфера ставати як однієї з найважливіших сфер міжнародного співробітництва, а й об'єктом суперництва. В даний час більшість керівників підприємств та організацій вживають заходів щодо «захисту та оборони» важливої для них інформації. Однак практика показує, що ці дії не завжди мають системний характер. В основному вони спрямовані на ліквідацію лише окремих загроз, залишаючи проломи в обороні.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

На жаль, в Україні досі відсутня єдина система безпеки підприємництва. Тому керівництву будь-якої організації доводиться самостійно вирішувати складне завдання забезпечення своєї економічної та інформаційної безпеки з оптимальними фінансовими втратами, але на необхідному рівні захищеності. з оптимальними фінансовими витратами, але на необхідному рівні захищеності.

Кожне підприємство та організація змушені постійно вести конкурентну боротьбу за своє існування, за прибуткове ведення справ, за своє добре ім'я в умовах становлення ринкової економіки. Успіх виробничої та підприємницької діяльності значною мірою залежить від уміння розпоряджатися таким цінним товаром, як інформація. Тому в умовах посилення конкуренції успіх підприємництва гарантія отримання прибутку все більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал та конкретну технологію.

Саме поняття «безпека» набуває розширеного змісту, воно включає питання інформаційно-комерційної, юридичної та фізичної безпеки, вирішення яких потребує особливої уваги у зв'язку зі зростаючою роллю інформації в житті суспільства.

Розглянемо фундаментальні поняття та визначення в галузі інформаційної безпеки та надійності систем:

Інформація – відомості (дані) про внутрішній і навколишній світ, події, процеси, явища тощо, сприймані та передані людьми або технічними пристроями.

Інформаційна (інформаційно-обчислювальна) система – організаційно впорядкована сукупність документів, технічних засобів та інформаційних технологій, що реалізує інформаційні (інформаційно-обчислювальні) процеси.

Інформаційні процеси – процеси збирання, накопичення, зберігання, обробки (переробки), передачі та використання інформації.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Інформаційні ресурси – окремі документи чи масиви документів в інформаційних системах.

Доступ – спеціальний тип взаємодії між об'єктом та суб'єктом, у результаті якого створюється потік інформації від одного до іншого.

Несанкціонований доступ (НСД) – доступ до інформації, пристроїв її зберігання та обробки, а також до каналів передачі, що реалізується без відома (санкції) власника і тим самим порушує встановлені правила доступу.

Об'єкт – пасивний компонент системи, що зберігає, переробляє, передає або приймає інформацію; приклади об'єктів: сторінки, файли, папки, директорії, комп'ютерні програми, пристрої (монітори, диски, принтери тощо).

Суб'єкт – активний компонент системи, котрий може ініціювати потік інформації; приклади суб'єктів: користувач, процес чи пристрій.

Безпека ІТТ – властивість системи, що виражається у здатності системи протидіяти спробам несанкціонованого доступу або заподіяння шкоди власникам та користувачам системи при різних навмисних та ненавмисних впливах на неї.

Захист інформації – організаційні, правові, програмно-технічні та інші заходи щодо запобігання загрози інформаційній безпеці та усунення їх наслідків.

Атака – спроба несанкціонованого подолання захисту системи.

Інформаційна безпека систем – властивість інформаційної системи або процесу, що реалізується в ній, що характеризує здатність забезпечити необхідний рівень свого захисту. Або інше визначення. Інформаційна безпека – всі аспекти, пов'язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності інформації або засобів її обробки:

Конфіденційність (confidentiality) – стан інформації, при якому доступ до неї здійснюють лише суб'єкти, які мають на неї право;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Цілісність (integrity) – уникнення несанкціонованої модифікації інформації;

Доступність (availability) – уникнення тимчасового чи постійного приховування інформації від користувачів, які отримали права доступу.

Цінність інформації визначається ступенем її корисності для власника. **Ідентифікація** – процес розпізнавання певних компонентів системи (об'єктів чи суб'єктів) за допомогою унікальних ідентифікаторів.

Аутентифікація – перевірка ідентифікації користувача або іншого компонента ІС для ухвалення рішення про дозвіл доступу до ресурсів системи.

Надійність системи – характеристика здатності програмного, апаратного, апаратно-програмного засобу виконати за певних умов необхідні функції протягом певного періоду часу. Достовірність роботи системи (пристрою) – властивість, що характеризує істинність кінцевого (вихідного) результату роботи (виконання програми), що визначається здатністю засобів контролю фіксувати правильність чи хибність роботи.

Помилка пристрою – неправильне значення сигналу (біта – у цифровому пристрої) на зовнішніх виходах пристрою або окремого його вузла, викликане технічною несправністю, або перешкодами, що впливають на нього (навмисними або ненавмисними), або іншим способом.

Помилка програми – проявляється у невідповідному реальному (потрібному) проміжному або кінцевому значенню (результату) внаслідок неправильно запрограмованого алгоритму або неправильно складеної програми.

Достовірність інформації визначається достатньою для власника точністю відображати об'єкти та процеси навколишнього світу у певних часових та просторових рамках. Інформація, що спотворено представляє дійсність, може завдати власнику значних матеріальних та моральних збитків. Якщо інформація спотворена навмисне, той її називають дезінформацією.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Комп'ютерний злочин надзвичайно багатогранне та складне явище. Об'єктами такого злочину можуть бути самі технічні засоби (комп'ютери та периферія) як матеріальні об'єкти або програмне забезпечення так і бази даних, для яких технічні засоби є оточенням; комп'ютер може бути предметом посягань чи інструмент.

Види викрадення персональних даних в соціальних мережах та месенджерах надзвичайно різноманітні. Це може бути несанкціонований доступ до інформації, що зберігається на пристрої користувача, так і введення в програмне забезпечення «логічних бомб», що можуть спрацювати при виконанні певної умови та частково або повністю вивести з ладу систему. Також необхідно врахувати той факт, що комп'ютерний злочин може статися також через недбалість у розробці, при виготовлянні та експлуатації програмно-обчислювальних комплексів.

Методів захисту інформації представлені на рис. 4.1

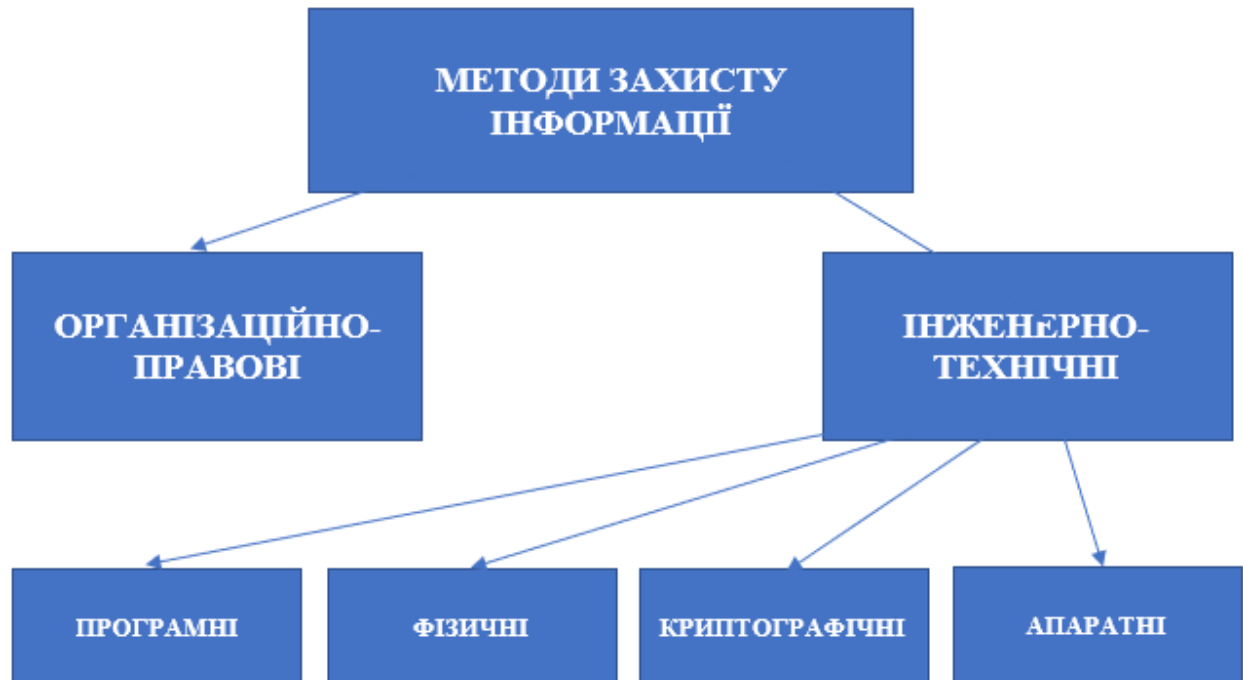


Рисунок 4.1 – Класифікація методів захисту інформації

До методів та засобів організаційного захисту інформації відносяться організаційно-технічні та організаційно-правові заходи, що проводяться у процесі створення та експлуатації КС для забезпечення захисту інформації. Дані заходи необхідно проводити при будівництві або ремонті приміщення, там де будуть розміщені комп'ютери.

Основою проведення організаційних заходів є використання та підготовка законодавчих та нормативних документів у галузі інформаційної безпеки, які на правовому рівні мають регулювати доступ до інформації з боку споживачів. У законодавстві пізніше, ніж у законодавстві інших розвинутих країн, виникли необхідні правові акти (хоча далеко ще не все).

Інженерно-технічний захист (ІТЗ) – це сукупність спеціальних технічних засобів та заходів щодо їх використання на користь захисту персональних даних.

Різновид цілей, завдань, об'єкту захисту та заходів, що проводяться, повинен передбачати розглядання деякої системи класифікації засобів за різними характеристиками, такими як вид, орієнтація та багато інших.

Наприклад, самі засоби ІТЗ можна розглядати щодо об'єктів їх впливу. У цьому плані може застосовуватися захист для людей, матеріальних засобів, фінансів, персональної інформації.

Різновид класифікованих характеристик дозволить розглядати ІТЗ засоби за об'єктами впливу, характерами заходів, способами реалізації, масштабом охоплення, класифікацією засобів зловмисників, яким буде здійснена протидія з боку служби безпеки України.

За функціональним призначенням засоби ІТЗ можна розділити на такі групи:

1. *Фізичні засоби.* Вони повинні включати різні засоби та споруди, що перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та до матеріальних носіїв конфіденційної інформації;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

2. *Апаратні засоби.* Ними є прилади або пристрої та інші технічні рішення, що використовуються у сфері захисту персональних даних. На практиці діяльності компаній знаходить широке застосування різна апаратура, починаючи з телефонного апарату до досконалих автоматизованих систем, що забезпечують роботу серверів. Основне їх завдання – забезпечити стійкий захист інформації від розголошення, витоку та несанкціонованого доступу через різні технічні засоби;

3. *Програмні засоби.* Повинні охоплювати спеціальні програми та програмні комплекси, що повинні забезпечити: збирання, накопичення, зберігання, обробку та передачу даних в соціальних мережах та месенджерах;

4. *Криптографічні засоби.* Спеціальні математичні та алгоритмічні засоби захисту інформації, що передається по системах і мережах зв'язку, що зберігається та обробляється на серверах, що використовують різноманітні методи шифрування.

3.7 Організаційно-правовий захист інформації

До технологій організаційного захисту відносяться організаційно-технічні та організаційно-правові заходи, що проводяться в процесі створення та експлуатації комп'ютерної системи для забезпечення захисту інформації.

Основні властивості технології організаційного захисту:

- забезпечення повного чи часткового перекриття значної частини каналів витоку інформації;
- об'єднання всіх використовуваних у комп'ютерній системі засобів у цілісний механізм захисту інформації.
- Технології організаційного захисту інформації включають:
- обмеження фізичного доступу до об'єктів комп'ютерної системи та реалізація режимних заходів;
- обмеження можливості перехоплення ПЕМІН;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

- розмежування доступу до інформаційних ресурсів та процесів комп'ютерної системи;
- резервне копіювання найважливіших з погляду втрати масивів документів;
- профілактику зараження комп'ютерними вірусами.

Перерахуємо основні види заходів, які мають проводитись на різних етапах життєвого циклу комп'ютерної системи:

- при розробці математичного, програмного, інформаційного та лінгвістичного забезпечення використання сертифікованих програмних та інструментальних засобів; при монтажі та налагодженні обладнання - контроль за роботою технічного персоналу; при випробуваннях та прийманні в експлуатацію - включення до складу атестаційних комісій сертифікованих спеціалістів;
- у процесі експлуатації комп'ютерної системи - організація пропускового режиму, визначення технології автоматизованої обробки документів, організація роботи обслуговуючого персоналу, розподіл реквізитів розмежування доступу користувачів до елементів комп'ютерної системи, організація ведення протоколів роботи комп'ютерної системи, контроль виконання вимог службових інструкцій тощо;
- заходи загального характеру - підбір та підготовка кадрів, організація планових та запобіжних перевірок засобів захисту інформації, планування заходів щодо захисту інформації, навчання персоналу, участь у семінарах, конференціях та виставках з проблем безпеки інформації тощо.

Основою проведення організаційних заходів є використання та підготовка законодавчих та нормативних документів у галузі інформаційної безпеки, які на правовому рівні мають регулювати доступ до інформації з боку споживачів.

Можна виділити чотири рівні правового забезпечення інформаційної безпеки. Перший рівень утворюють міжнародні договори, до яких приєдналася Україна, та українське законодавство:

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

міжнародні конвенції про охорону промислової власності, охорону інтелектуальної власності, авторське право;

ЦК України (в ст. 139 встановлюється право на відшкодування збитків від витоку за допомогою незаконних методів інформації, що відноситься до службової та комерційної таємниці);

КК України (ст. 272 встановлює відповідальність за неправомірний доступ до комп'ютерної інформації, ст. 273 – за створення, використання та розповсюдження шкідливих програм для ЕОМ, ст. 274 – за порушення правил експлуатації ЕОМ, систем і мереж);

Другий рівень правового забезпечення інформаційної безпеки становлять підзаконні акти, до яких належать укази Президента України та постанови Верховної Ради України, а також листи Верховного Суду України та постанови Господарського та Апеляційного судів.

Третій рівень правового забезпечення інформаційної безпеки становлять державні стандарти (ДСТУ) у сфері захисту інформації, керівні документи, норми, методики та класифікатори, розроблені відповідними державними органами. Наприклад:

ДСТУ 50922-96 «Захист інформації. Основні терміни та визначення», ДСТУ 50739-95 «Засоби обчислювальної техніки. Захист від несанкціонованого доступу до інформації. Загальні технічні вимоги, ДСТУ «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» та ін;

також керівні документи Державної технічної комісії при Президенті України та Міністерства Цифрової Трансформації України «Концепція захисту засобів обчислювальної техніки та автоматизованих систем від несанкціонованого доступу до інформації», «Автоматизовані системи. Захист від несанкціонованого доступу до інформації. Класифікація автоматизованих систем та вимоги щодо захисту інформації» та ін.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Четвертий рівень правового забезпечення інформаційної безпеки утворюють локальні нормативні акти, положення, інструкції, методичні рекомендації та інші документи щодо комплексного захисту інформації у комп'ютерній системі конкретної організації. До таких нормативних документів належать:

- наказ про затвердження переліку відомостей, що становлять комерційну таємницю підприємства;
- трудові та цивільно-правові договори, до яких включені пункти про обов'язок відшкодування збитків за розголошення відомостей, що становлять комерційну таємницю підприємства, та ін.

3.8 Інженерно-технічний захист інформації

Інженерно-технічний захист - це сукупність спеціальних органів, технічних засобів та заходів щодо їх використання на користь захисту конфіденційної інформації. Класифікація видів інженерно-технічної інформації наведено на рис. 4.2.

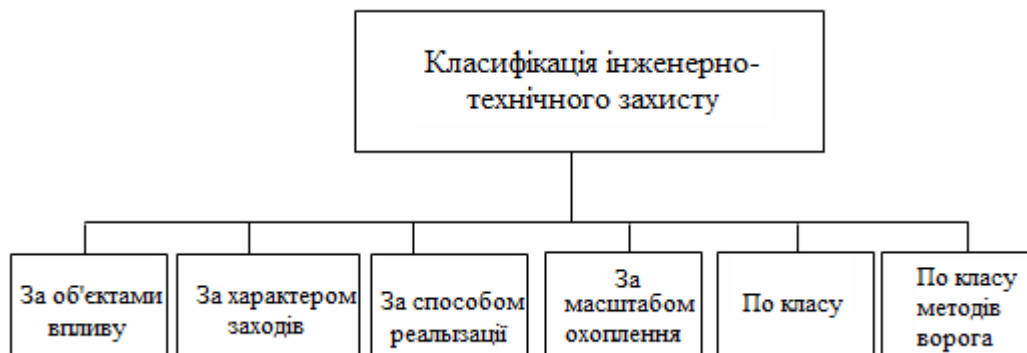


Рисунок 4.2 – Класифікація видів інженерно-технічної інформації

За функціональним призначенням засоби інженерно-технічного захисту класифікуються на наступні групи:

1. фізичні засоби – включають в себе різноманітні засоби та споруди, які є перешкодою на фізичному рівні доступу злоумисника на об'єкт захисту та

до матеріальних носіїв конфіденційної інформації. Також, здійснюють захист персоналу, матеріальних засобів та фінансів від протиправних впливів.

До цього класу засобів захисту відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- та радіотехнічні та інші пристрої для заборони злочинних дій. Усі фізичні засоби захисту об'єктів можна поділити на три категорії:

- а) засоби попередження (охоронна сигналізація);
- б) засоби виявлення (відео системи, СКУД);
- с) системи ліквідації загроз (замикаючі пристрої).

2. апаратні засоби - прилади, пристрої, пристрої та інші технічні рішення, що використовуються в інтересах захисту інформації. Завдання апаратних засобів полягає в забезпеченні стійкого захисту інформації від розголошення, витоку та несанкціонованого доступу через технічні засоби, що застосовуються у виробничій діяльності;

3. програмні засоби - спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різного призначення та засобах обробки даних;

4. криптографічні засоби - спеціальні математичні та алгоритмічні засоби захисту інформації, що передається за системами та мережами зв'язку, що зберігається та обробляється на ЕОМ з використанням різноманітних методів шифрування.

3.9 Фізичні методи та засоби захисту інформації.

Фізичні засоби захисту - це різновид пристроїв, конструкцій, апаратів, виробів, що в свою чергу призначені для створення перешкод на шляху зловмисників.

До фізичних засобів необхідно віднести механічні, електромеханічні, електронні, електронно-оптичні, радіо- та радіотехнічні пристрої для заборони несанкціонованого доступу (входу, виходу).

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

Ці засоби використовуються для вирішення таких завдань:

- 1) охорона території розташування серверів компаній та спостереження за цією територією;
- 2) охорона будівлі та внутрішніх приміщень;
- 3) охорона обладнання, продукції, фінансів та інформації;
- 4) застосування способів контролю доступу до будівлі та приміщень.

Всі фізичні засоби захисту об'єктів можна поділити на такі категорії:

- засоби попередження;
- засоби виявлення
- системи ліквідації загроз.

Охоронну сигналізацію та відеонагляд можна віднести до засобів виявлення загроз; паркан навколо об'єкту захисту – це засіб запобігання несанкціонованому проникненню на територію. Засоби пожежогасіння належать до системи ліквідацій загроз.

3.10 Апаратні методи та засоби захисту інформації.

До цих засобів захисту можна віднести різноманітні за принципом дії, що забезпечать припинення, розголошення, захист від витоку та протидії несанкціонованому доступу до джерел конфіденційної інформації.

Апаратні засоби захисту використовують для вирішення таких завдань:

- 1) проведенню досліджень технічних засобів забезпечення на існування можливих каналів витоку інформації;
- 2) виявити канали витоків інформації на об'єкті та в приміщеннях;
- 3) локалізувати канали витоку інформації;
- 4) пошук та виявлення засобів промислового шпигунства;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

- 5) протидії несанкціонованому доступу до джерел інформації та інших дій.

3.11 Програмні методи та засоби захисту інформації

Системи захисту комп'ютера від чужого вторгнення дуже різноманітні та класифікуються, як:

- 1) засоби власного захисту, передбачені загальним програмним забезпеченням;
- 2) засоби захисту у складі обчислювальної системи;
- 3) засоби захисту із запитом інформації;
- 4) засоби активного захисту;
- 5) засоби пасивного захисту та інші.

Можна виділити такі напрямки використання програм для забезпечення безпеки конфіденційної інформації, зокрема такі методи захисту:

1. інформації від несанкціонованого доступу;
2. інформації від копіювання;
3. програм від копіювання;
4. програм від вірусів;
5. інформації від вірусів;
6. програмний каналів зв'язку.

Програмні засоби захисту мають такі різновиди спеціальних програм:

- 1) ідентифікації технічних засобів, файлів та автентифікації користувачів;
- 2) реєстрації та контролю роботи технічних засобів та користувачів;
- 3) обслуговування режимів обробки інформації обмеженого користування;
- 4) захисту операційних засобів ЕОМ та прикладних програм користувачів;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

- 5) знищення інформації у захисні пристрої після використання;
- 6) сигналізують порушення використання ресурсів;
- 7) допоміжні програми захисту різного призначення.

Захист інформації від несанкціонованого доступу

Для забезпечення захисту від вторгнень необхідно передбачити заходи безпеки. Основні функції, що повинні здійснювати ПЗ, це:

- 1) ідентифікації суб'єктів та об'єктів;
- 2) розмежування (або ізоляція) доступу до обчислювальних ресурсів та інформації;
- 3) здійснення контролю та реєстрації дій з інформацією та програмами.

Захист від копіювання.

Впровадження засобів захисту від копіювання може запобігти використанню викрадених копій ПЗ. Під цими засобами захисту розуміють засоби, що забезпечують виконання програмою своїх функцій лише за впізнанням деякого унікального некопійованого елементу. Таким елементом (ключем) може бути флешка, певна частина комп'ютера або спеціальний пристрій, що підключається до персонального комп'ютера. Захист від копіювання реалізується виконанням ряду функцій, які є спільними для всіх систем захисту:

1. Ідентифікація середовища, з якого буде запущена програма (флешка або ПК);
2. Автентифікація середовища, з якого запущена програму;
3. Дія на запуск із несанкціонованого середовищу;
4. Реєстрація санкціонованого копіювання;
5. Протидії вивченню алгоритмів роботи системи.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

Захист програм та даних від комп'ютерних вірусів

Шкідливі програми, такі як віруси становлять серйозну небезпеку при зберіганні конфіденційної інформації. Недооцінка цього фактору може викликати серйозні наслідки інформації користувачів.

«Комп'ютерні віруси» –виконувані або інтерпретовані програми, що можуть розповсюджуватися та само відтворюватися (реплікація) у комп'ютерній системі. Віруси в основному виконують заміну або знищують ПЗ або дані. В процесі розповсюдження віруси також мають властивість до модифікації.

Класифікація комп'ютерних вірусів

Усі комп'ютерні віруси можуть бути класифіковані за такими ознаками:

- серед існування вірусу,
- за способом зараження довкілля,
- за деструктивними можливостями,
- за особливостями алгоритму вірусу.

Виявлення вірусів бажано здійснювати на стадії їх впровадження або принаймні до початку здійснення деструктивних функцій вірусів. Слід зазначити, що немає антивірусних засобів, які гарантують виявлення всіх можливих вірусів.

При виявленні вірусу необхідно відразу припинити роботу програми-вірусу, щоб мінімізувати збитки від нього на систему.

Усунення наслідків впливу вірусів ведеться у двох напрямках:

- Видалення вірусів,
- Відновлення (за необхідності) файлів, областей пам'яті.

Для боротьби з вірусами використовуються програмні та апаратно-програмні засоби, які застосовуються у певній послідовності та комбінації, утворюючи методи боротьби з вірусами.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

Найнадійнішим методом захисту від вірусів є використання апаратно-програмних антивірусних засобів.

Апаратно-програмні антивірусні засоби мають ряд переваг перед програмними:

- працюють постійно;
- виявляють усі віруси, незалежно від механізму їхньої дії;
- блокують недозволені дії, які є результатом роботи вірусу або некваліфікованого користувача.

Сучасні програмні антивірусні засоби можуть здійснювати комплексну перевірку комп'ютера щодо виявлення комп'ютерних вірусів. Для цього використовуються такі антивірусні програми як Kaspersky Anti-Virus (AVP), Norton Antivirus, Dr. Web, Symantec Antivirus. Усі вони мають антивірусні основи, які періодично оновлюються.

3.12 Криптографічні методи та засоби захисту інформації

Криптографія як засіб захисту (закриття) інформації набуває все більш важливого значення у світі комерційної діяльності.

Криптографія є сукупність методів, які спрямовані на те, щоб зробити дані марними для зловмисника. Такі перетворення дозволяють вирішити два головні питання щодо безпеки інформації:

- захист конфіденційності;
- захист цілісності.

Класифікація методів криптографічного перетворення інформації показана на рис. 4.3.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		76



Рисунок 4.3 – Класифікація методів криптографічного перетворення інформації

Процеси шифрування даних полягають у проведенні математичного, логічного, комбінаторного та інших перетворень вихідної інформації. В результаті цього зашифровується інформація та виглядає як хаотичний набір букв, цифр та інших наборів символів або у вигляді двійкового коду.

Для шифрування інформації найчастіше використовують один або декілька алгоритмів перетворення та ключ. Вихідними даними для алгоритму шифрування є інформація, яку необхідно шифрувати, та ключ шифрування. Ключ містить інформацію, що визначає вибір перетворення на певних етапах алгоритму та величини операндів, які використовуються при шифрування інформації. Операнд - це константа, змінна, функція, вираз та інший об'єкт мови програмування, над яким виконуються операції.

На відміну від інших, методи стеганографії дозволяють приховати не тільки зміст інформації, що зберігається або передається, але і сам факт зберігання або передачі закритої інформації. У реалізації методу стеганографії лежить – маскування закритої інформації серед відкритих файлів. Обробка мультимедійних файлів в інформаційних системах відкрила майже необмежені можливості перед стеганографією.

Користуючись засобами стеганографії можна маскувати текст, зображення, мову, цифровий підпис, зашифроване повідомлення.

Прихований файл також може бути зашифровано. Навіть, якщо хтось виявить прихований файл, то зашифрована в ньому інформація може сприйнятися як збій у роботі системи.

Змістом процесу кодування інформації є заміна вихідного змісту повідомлення (слів, речень) кодами. Як коди можуть використовуватися поєднання букв, цифр, знаків. При кодуванні та зворотному перетворенні використовуються спеціальні таблиці або словники. В інформаційних мережах кодування вихідного повідомлення (або сигналу) програмно-апаратними засобами застосовується для підвищення достовірності інформації, що передається.

Часто кодування і шифрування помилково приймають за те й теж, забувши у тому, що з відновлення закодованого повідомлення, досить знати правило заміни, тоді як розшифровки повідомлення крім знання правил шифрування, потрібен ключ до шифру.

Стиснення інформації можна віднести до методів криптографічного перетворення інформації з певними застереженнями. Метою даного методу є скорочення обсягу інформації. У той же час, стиснена інформація не може бути прочитана або використана без зворотного перетворення. Враховуючи доступність засобів стиснення та зворотного перетворення, ці методи не розглядаються як надійні засоби криптографічного перетворення інформації.

Основним видом криптографічного перетворення інформації у мережах є шифрування. Шифрування – процес перетворення відкритої інформації на зашифровану (шифртекст) або навпаки.

Методом шифрування (шифром) називається сукупність оборотних перетворень відкритої інформації у закриту інформацію відповідно до алгоритму шифрування.

Атака на шифр (криптоаналіз, криптоатака) – це процес розшифрування закритої інформації без знання ключа та, можливо, за відсутності відомостей про алгоритм шифрування.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

Сучасні методи шифрування обов'язково мають відповідати таким вимогам:

- стійкість шифру протистояти криптоаналізу (криптостійкість) повинна бути такою, щоб розтин його могло бути здійснено лише шляхом здійснення повного перебору ключів;
- криптостійкість забезпечується не секретністю алгоритму шифрування, а секретністю ключа;
- шифртекст нічого не винні істотно перевищувати за обсягом вихідну інформацію;
- помилки, що виникають при шифруванні, не повинні призводити до спотворень та втрат інформації;
- час шифрування має бути великим;
- вартість шифрування повинна бути погоджена з вартістю інформації, що закривається.

Криптостійкість шифру є його основним показником ефективності. Вона вимірюється часом або вартістю коштів, необхідних криптоаналітику для отримання вихідної інформації з шифртексту, за умови, що невідомий ключ.

Зберегти в секреті алгоритм шифрування, що широко використовується, практично неможливо. Тому алгоритм повинен мати прихованих слабких місць, якими могли б скористатися криптоаналітики. Якщо ця умова виконується, то криптостійкість шифру визначається довжиною ключа, тому що єдиний шлях розкриття зашифрованої інформації – перебір комбінацій ключа та виконання алгоритму розшифрування. Таким чином, час та засоби, що витрачаються на криптоаналіз, залежать від довжини ключа та складності алгоритму шифрування.

3.13 Об'єкти захисту

Об'єкт захисту є десятиповерховий будинок, що знаходиться на огороженій по периметру території. Праворуч і ліворуч є гранична територія сторонніх

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

компаній із суміжними кордонами. Крім будівлі на території є місце паркування автомобілів.

Зона розташування об'єкта захисту інформації знаходиться на п'ятому поверсі вказаної будівлі. У контрольовану зону входять такі об'єкти та приміщення:

- кабінет для проведення нарад;
- кабінет керівника;
- серверна;
- прилади та техніка, система обробки, зберігання та передачі даних.

Фізико-технічні характеристики приміщень мають такі властивості:

Стіни зовнішні:

- *Матеріал: залізобетонні;*
- *Товщина (0,8 м);*
- *Екранування та штукатурка: присутній;*
- *Інші матеріали: з внутрішньої сторони стіни оздоблені під "Євро-стандарт".*

Вікна:

- *Розмір отвору: 2,0 * 1,5 м;*
- *Тип вікна: склопакет із подвійним потовщеним склом.*

Двері:

- *Розмір отвору: 2,2*1,8м*
- *Тип: одностулкові, металеві двері, замок механічний.*

Система вентиляції:

- *Припливно-витяжна.*

Система опалення:

- *Центральне водяне.*

Система електроживлення (освітлення):

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

- Мережа: 220 В/50 Гц;
- Тип світильників: галогенні стельові світильники

Система заземлення:

- відсутня;

Телефонні лінії:

- Тип ТА.

Контрольована зона - це територія об'єкта, де виключено неконтрольоване перебування осіб які мають постійного чи разового доступу. Контрольована зона може обмежуватися периметром територією, що охороняється частково, територією, що охороняється, охоплює будівлі та споруди, в яких проводяться закриті заходи, частиною будівель, кімнати, кабінети, в яких проводяться закриті заходи.

Контрольована зона може встановлюватися більш ніж територія, що охороняється, при цьому забезпечує постійний контроль за не охороняється частиною території. Постійна контрольована зона - це межа, якої встановлюється на тривалий термін. Тимчасова зона - це зона, яка встановлюється щодо закритих заходів разового характеру.

Відповідно до нормативних документів об'єкти діляться на універсальні об'єкти, які у свою чергу поділяються на три категорії:

- першої категорії універсального об'єкта, що вимагає 50 метрів контрольованої зони;
- другий категорії об'єкта, потрібно 30 метрів;
- третій категорії об'єктів потрібно 15 метрів контрольованої зони.

Аналізований об'єкт відноситься до другої категорії з радіусом контрольованої зони, що дорівнює тридцяти метрам.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

3.14 Планування та реалізація систем захисту

Головною причиною появи безпекової політики зазвичай є вимога наявності такого документа від регулятора - організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності. Крім того, певні вимоги (рекомендації) висувають галузеві чи загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається як зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства.

Відсутність політики викликає негативну оцінку, яка впливає на публічні показники підприємства - позиції в рейтингу, рівень надійності.

На основі виявлених недоліків у захисті системи передачі даних розроблено таку політику безпеки мережі:

Аудит - розділ, присвячений аудиту в безпековій політиці, визначає типи подій, що відстежуються у всіх системах. Стандартними подіями є такі:

- спроби входу в систему управління інформаційною безпекою мережі (успішні або невдалі);
- вихід із системи;
- помилки доступу до файлів або системних об'єктів;
- спроби віддаленого доступу (успішні чи невдалі);
- дії привілейованих користувачів (адміністраторів), успішні чи невдалі;
- системні події (вимикання та перезавантаження).

Кожна подія повинна включати таку інформацію:

- ID користувача (якщо є);
- дата і час;
- ID процесу (якщо є);
- виконану дію;
- успішне чи невдале завершення події.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

У політиці безпеки, що розробляється, встановлюється термін і спосіб зберігання записів аудиту. По можливості вказується спосіб та частота перегляду цих записів. Багато організаціях застосовується політика тривалого зберігання інформації. Перед розробкою безпекової політики уважно ознайомтеся з існуючими правилами, щоб у різних політиках не було схожих вимог.

У цій політиці мережевої безпеки для кожного типу з'єднань у мережі політика безпеки визначає правила встановлення мережових з'єднань та використовувані механізми захисту:

- З'єднання набірного доступу. Вимоги до цих сполук встановлюють технічні правила автентифікації, включаючи автентифікаційні правила для кожного типу з'єднання. Вони викладаються у розділі автентифікації політики і можуть встановлювати сильніші методи автентифікації, ніж звичайні. Крім того, у політиці визначаються вимоги до автентифікації при отриманні доступу через набірний з'єднання. Для організації доцільно встановити суворий контроль над дозволеними точками доступу, щоб дотримуватися вимог авторизації в мережі;

- Виділені лінії. У організаціях використовуються різні типи виділених ліній, і кожного типу необхідно визначити пристрої захисту. Найчастіше такі пристрої є міжмережевими екранами. Тільки вказівка типу пристрою сама по собі не передбачає будь-якого рівня захисту. Політика безпеки повинна визначати базову політику контролю доступу, що застосовується на пристрої, а також процедуру запиту та отримання доступу, яка не є частиною стандартної конфігурації;

- Віддалений доступ до внутрішніх систем. Нерідко організації дозволяють своїм співробітникам здійснювати доступ до внутрішніх систем із зовнішніх віддалених місць. Політика безпеки повинна визначати механізми, які використовуються під час здійснення такого доступу. Необхідно вказати, щоб усі з'єднання були захищені шифруванням, визначити специфіку, пов'язану з типом шифрування. Оскільки підключення здійснюється ззовні організації, рекомендується використовувати надійний механізм автентифікації. Крім того,

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

політика безпеки має визначати процедуру проходження авторизації для такого доступу. Бездротові мережі. Бездротові мережі стають популярними, і установка у підрозділі бездротового зв'язку без відома відділу інформаційних технологій вже стала звичайною справою. Політика безпеки повинна визначати умови, за яких дозволяється використання бездротових з'єднань, і те, яким чином здійснюватиметься авторизація в такій мережі. Якщо використовується бездротова мережа, необхідно вказати додаткові вимоги до автентифікації або шифрування. Бездротові мережі слід розглядати як зовнішні незахищені мережі, а не як частину внутрішньої мережі організації. Якщо так і є насправді, цей факт має бути помічений у політиці.

3.15 Методи захисту інформації

Базовими елементами політики у сфері безпеки є ідентифікація, цілісність та активна перевірка.

Ідентифікація покликана запобігти загрозі знеособлення та несанкціонованого доступу до ресурсів та даних. Цілісність забезпечує захист від підслуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність інформації, що передається. І нарешті, активна перевірка (аудит) означає перевірку правильності реалізації елементів політики безпеки та допомагає виявляти несанкціоноване проникнення в мережу та атаки. а DoS.

Механізми ідентичності потрібно впроваджувати обережно, т. я. навіть найкраще продумана політика може бути невдала, якщо складно використовувати удосконалення. Класичним прикладом є запис пароля на клаптику паперу і прикріплення його до монітора комп'ютера - що є виходом для споживача, який повинен пам'ятати безліч паролів для отримання доступу до складових частин мережі, що змінюються. Обтяжливі або надмірно дубльовані системи верифікації та авторизації можуть засмутити користувачів, тому їх слід уникати. Методи

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

ідентифікації можуть ґрунтуватися на протоколі S/Key або здійснюватись за допомогою спеціальних апаратних засобів (token password authentication). А серед модемного доступу часто застосовується механізм ідентифікації за протоколом Point-to-Point Protocol (PPP), який включає використання протоколів Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) і Extensible Authentication Protocol (EAP).

Цілісність – це елемент, який включає безпеку пристрою інфраструктури мережі (фізичний та логічний доступ), безпеку периметра та конфіденційність даних. Безпека фізичного доступу може виражатися у розміщенні обладнання мережі у спеціально створених для цього обладнання шафах, які мають обмежений доступ.

Безпека логічного доступу головним чином стосується забезпечення механізмів ідентичності (ідентифікації та авторизації) перед тим, як дати доступ до мережі зв'язку Telnet або терміналу до компонентів інфраструктури загальної мережі (наприклад, маршрутизаторів або міжмережевих екранів). Безпека периметра пов'язана з функціями міжмережевих екранів, що визначають, який трафік дозволено або заборонено від різних зон мережі, зазвичай між мережею Інтернет і головним комплексом або між користувачами віддаленого доступу і головним комплексом.

Конфіденційність даних може забезпечуватися протоколами безпеки на транспортному рівні SSL та Secure Shell Protocol (SSH), які здійснюють безпечну передачу даних між клієнтом та сервером. Безпечний протокол передачі гіпертексту (S-HTTP) надає надійний механізм Web-транзакцій, проте найпопулярнішим засобом є SSL. Засіб SOCKS є рамковою структурою, що дозволяє програмам клієнт/сервер у доменах TCP та UDP зручно та безпечно користуватися послугами мережного міжмережевого екрану. Протокол безпеки IP (IPSec) є набір стандартів підтримки цілісності та конфіденційності даних на мережевому рівні (у мережах IP). X.509 є стандартом безпеки та ідентифікації, що підтримує структури безпеки електронного інформаційного транспорту.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

Останнім головним елементом системи безпеки є аудит, який необхідний для стеження та верифікації процесу дослідження політики безпеки. Для випробування ефективності інфраструктури системи безпеки аудит безпеки повинен відбуватися часто, через рівні проміжки часу. Він також повинен включати перевірки установки нової системи, методи для визначення можливої шкідницьких дій будь-кого з внутрішнього персоналу та можливої наявності особливого класу проблем (напади типу «відмова у сервісі»), а також загальне дотримання політики безпеки об'єкта.

При розробці політики безпеки необхідно враховувати вимогу збалансувати легкість доступу до інформації та адекватний механізм ідентифікації дозволеного користувача та забезпечення цілісності та конфіденційності даних. Політика безпеки повинна запровадитися примусово як технічно, так і організаційно – тоді вона буде по-справжньому ефективна.

Таким чином, для посилення інформаційної безпеки системи передачі даних об'єкта, що аналізується, необхідне виконання наступних дій:

- впровадження в існуючу мережу ключових елементів - для управління адресацією;
- здійснити розмежування даної мережі на сектори, що представляють сервери зберігання інформації, поштових серверів, мереж роботи користувачів, web-сервер, віртуальний приватний канал віддаленого зв'язку та виходу в інтернет;
- докладне вивчення характеристик маршрутизаторів компанії Cisco для оптимального вибору центрального маршрутизатора системи управління інформаційною безпекою мережі;
- у ключових сегментах мережі проводиться впровадження інтелектуальних маршрутизаторів компанії CISCO;
- здійснюється персональна конфігурація маршрутизаторів кожного сегмента мережі;

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

- вибір та налаштування програмного забезпечення для захисту даних, що передаються. Налаштування Outpost Firewall Pro.

3.16 Розробка захисту для основних активів компанії

Для вирішення завдання забезпечення інформаційної безпеки було обрано систем QBE_Systems, QBE_Systems — унікальне крос-функціональне рішення для автоматизації та управління доступом до інформаційних ресурсів компанії та контролю за дотриманням політики безпеки. QBE_Systems призначений для великих компаній з великою, різномірною КІС, з географічно розгалуженою структурою, що мають велику кількість щоденних кадрових операцій та/або високу ціну будь-яких помилок, пов'язаних із неправильно наданими правами доступу до інформаційних ресурсів. QBE_Systems дозволяє автоматизувати управління обліковими записами, реалізувати процес узгодження прав доступу, а також забезпечити безперервний моніторинг їх змін.

QBE_Systems - єдина на ринку України система, яка вирішує завдання одразу трьох основних груп користувачів:

1. Бізнес-підрозділів. Можливість самостійно у звичній термінології запитувати, погоджувати та отримувати доступ до необхідних інформаційних ресурсів через web-портал; будь-якої миті часу бачити поточний статус своєї заявки.

2. Служба інформаційних технологій/автоматизації. Можливість отримувати чіткі інструкції до виконання у зрозумілих виконавцю термінах; не витрачати час на уточнення вимог заявок; бути впевненим, що своїми діями інженер не порушує політику інформаційної безпеки компанії. Можлива повна автоматизація виконання заявок.

3. Служба інформаційної безпеки. можливість безперервно контролювати всі зміни прав доступу до інформаційних ресурсів компанії та інші зміни значимих налаштувань; мати всю необхідну інформацію для оперативного розслідування інцидентів, пов'язаних із недотриманням правил безпекової політики.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

Можливості QBE_Systems

1. Управління:

- Електронний документообіг заявок, електронний підпис та політики їх погодження;
- Рольова модель управління;
- Інструменти аналізу та оптимізації ролей;
- Гнучка система звітів для різних категорій користувачів.

2. Безпека:

- Відповідність внесених змін прав доступу до встановленої політики ІБ;
- Безперервний контроль несанкціонованих змін прав доступу;
- Узгоджене управління логічним та мережним доступом;
- Управління цифровими сертифікатами та контроль програмно-апаратних конфігурацій.

3. Автоматизація:

- Динамічна побудова маршрутів погодження заявок на зміну прав доступу;
- Управління обліковими даними та правами доступу користувачів на основі кадрових змін;
- Автоматична генерація інструкцій на зміну прав доступу або автоматичне виконання інструкцій.

Типова архітектура вирішення завдань управління доступом представлена на рис. 3.4.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

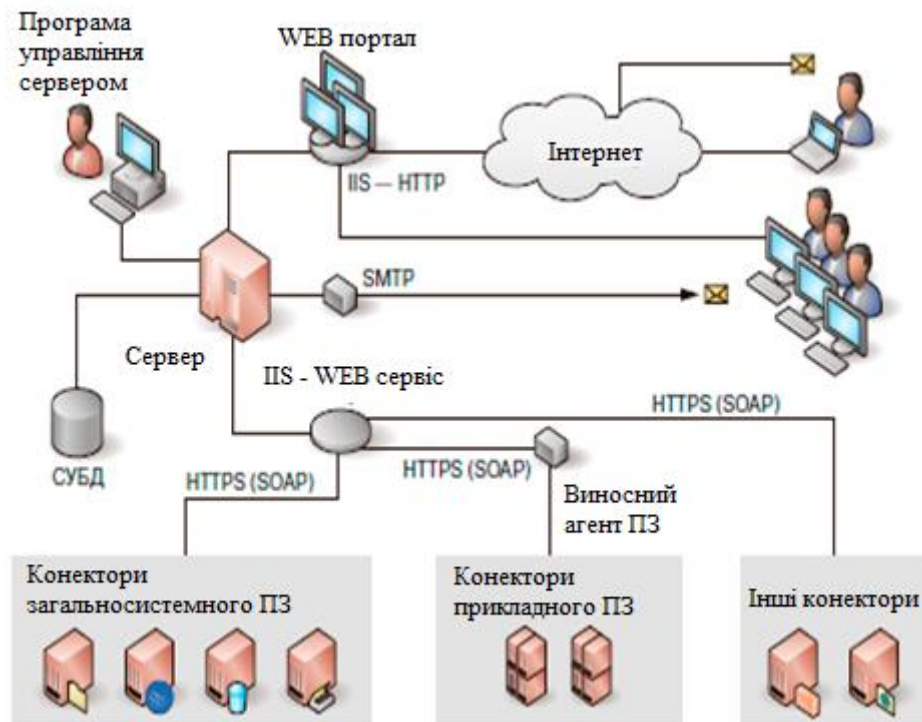


Рисунок 4.4 – Типова архітектура управління доступом

QBE_Systems має такі переваги:

1. Забезпечення безпеки. QBE_Systems – єдина система, що повністю вирішує завдання забезпечення інформаційної безпеки компанії на додаток до функціональності типової IDM. Крім управління логічним доступом, QBE_Systems забезпечує управління мережним доступом, цифровими сертифікатами та контроль програмно-апаратних конфігурацій. QBE_Systems здійснює безперервний контроль відповідності запитаних та реалізованих прав доступу.

2. Розслідування інцидентів. Зберігання повної історії всіх змін прав користувачів відкриває перед службою безпеки широкі можливості оперативного та ефективного розслідування інцидентів, пов'язаних з порушенням політики безпеки компанії. У QBE_Systems реалізовано захист електронних заявок та операцій, що виконуються з ними (створення, погодження, відхилення) за допомогою електронно-цифрового підпису.

3. Оптимізація технічних ресурсів. Логіка роботи інформаційних систем у QBE_Systems закладається у процесі налаштування, завдяки чому QBE_Systems

		Литвинюк В.С.			KIK.KP.B – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

може оперативно виявляти несанкціоновані зміни. Можливість автоматичного виконання заявок на зміну доступу дозволяє оптимізувати роботу технічних відділів і мінімізувати помилки, пов'язані з людським фактором.

4. Навчання та підтримка клієнтів. У постачання QBE_Systems входить докладна документація українською мовою. Для клієнтів працює гаряча підтримка. Ми навчаємо наших клієнтів у спеціалізованих навчальних центрах.

5. Розвиток. Гнучка архітектура системи QBE_Systems забезпечує широкі можливості щодо розширення функціональності та інтеграції із зовнішніми системами. Система швидко розвивається назустріч вимогам ринку. У кожній версії QBE_Systems з'являються нові унікальні можливості.

В результаті аудиту інформаційної безпеки підприємства було виявлено основні проблеми системи відеоспостереження. Враховуючи вищевикладене, розроблені заходи підвищення ефективності функціонування системи відеоспостереження організації:

- Заміна застарілих відеокамер.
- Встановлення камер у приміщеннях та на прилеглий території.
- Заміна монітора відеооператора.
- Встановлення сервера в окремому приміщенні.
- Встановлення відеомонітора біля прохідної.
- Заміна програмного забезпечення виведення відеосигналу.
- Заміна кабелю.

Завдяки запропонованим заходам буде побудовано ефективну систему відеоспостереження в організації. Розглянемо докладніше, що включатимуть запропоновані заходи.

1. Заміна застарілих камер.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

Термін служби електронних компонентів системи охоронного телебачення становить близько 7 років. У кабінеті директора та на прохідній використовуються камери виробника MinTron. На підставі документації про монтаж системи відеоспостереження закуплені камери були не новими. Вже використовувалися раніше, тобто. термін їхньої служби може бути більше 7 років.

Для заміни відеокамер вибрано камери серії KPC-190. Відеокамери серії KPC-190 мають підвищену чутливість і роздільну здатність.

2. Встановлення камер у приміщеннях.

Вирішено вибрати телекамеру KPC-S20. Відеокамери серії KPC-S20 мають підвищену чутливість і роздільну здатність. Ця модель відеокамери зарекомендувала себе як дуже надійна та невибаглива. Вона здатна дати чітке і контрастне зображення і має дуже малі габарити. Виробник фірми KT&C (Корея). Камера близька до своїх характеристик камерам серії KPC-400. Основна відмінність - це менші розміри, але дещо вища ціна. Між собою відеокамери серії KPC-S20 відрізняються об'єктивами та чутливістю. У комплекті з камерою входить П-подібний кронштейн

3. Вибір відеокамери для захисту периметра.

При модернізації системи відеоспостереження периметра необхідно усунути врахувати проблеми.

Неналежний захист камер від умов зовнішнього середовища.

Підвищення інформативності зображення камер, що спостерігають за вїздом на територію школи.

Для захисту камери від морозу, опадів та інших несприятливих умов. Можливе використання кожухів для стандартних безкорпусних камер або використання готових вуличних камер, які вже укомплектовані термокожухом.

Вуличні відеокамери спостереження були розроблені на основі термокожуха Модельний ряд вуличних камер відеоспостереження AS-1 включає моделі

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

з кутами огляду від 25 до 115 градусів, що дозволяє вирішувати більшість завдань, пов'язаних із забезпеченням вуличного відеоспостереження на будь-якому об'єкті.

Камери відеоспостереження AS-1 мають високу чутливість в інфрачервоному діапазоні та можуть використовуватись спільно з ІЧ-прожектором. Завдяки використанню додаткового фільтра можливе підключення декількох камер до одного джерела живлення. Приємний дизайн і колірне рішення відеокамер з використанням епоксиполіефірної фарби, що сприяє відображенню сонячних променів, що захищає камери від перегріву.

Для точок відеоспостереження, у яких покликане забезпечувати високу якість зображення та ідентифікацію деяких деталей. Вирішено використовувати відеокамеру того ж модельного ряду, але з більш високою роздільною здатністю AS-4.

4. Заміна монітора відеооператорів.

Для комфортного відеоспостереження в системі відеоспостереження слід замінити старий монітор.

Вибираючи тип монітора слід віддати перевагу РК-монітору. В основі того, що РК-монітор приємніший для очей лежить наступне:

— Відсутнє мерехтіння, властиве ЕПТ у зв'язку з постійним перемальовуванням екрана. На РК-дисплеї пікселі займають строго певне, фіксоване положення, і їх колір змінюються тільки в тому місці екрана, де на "картинці" відбувається рух.

— Жодних проблем пов'язаних зі зведенням променів. У кольорового ЕЛТ-монітора не одна, а три гармати, кожна на свій колір, і які посилюють кожна по променю, виникає проблема налаштувань з відомим і фокусуванням променів, ідеально нічого не буває, а тому знову страждає на якість зображення. У РК-моніторі кожен піксель розташований у фіксованій матриці та знає своє місце.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

– Бліків на екрані РК монітора в кілька разів менше. Коефіцієнт відбиття світла від поверхні РК монітора в три і більше разів менше, ніж від поверхні кінескопа з найдосконалішим на сьогоднішній день покриттям антивідблиску (Sony FD нфіденційно, Конфіденційно, суворо конфіденційно, а кожному користувачеві – рівень допуску. Доступ здійснюється за результатами порівняння рівня допуску з категорією конфіденційності інформації.

За допомогою засобів апаратної підтримки можна заборонити користувачеві завантаження ОС із зовнішніх знімних носіїв. Як апаратна підтримка система Secret Net 12 використовує програмно-апаратний комплекс Secret Net Touch Memory Card. Плату апаратної підтримки неможливо обійти засобами BIOS: якщо протягом певного часу після включення живлення на плату не було передано керування, вона блокує роботу всієї системи.

Контроль цілісності використовується для стеження за незмінністю контрольованих об'єктів з метою захисту від модифікації. Контроль проводиться в автоматичному режимі відповідно до певного розкладу.

Об'єктами контролю можуть бути файли, каталоги, елементи реєстру та сектори дисків. Кожен тип об'єктів має свій набір контрольованих параметрів. Так, файли можуть контролюватись на цілісність вмісту, прав доступу, атрибутів, і навіть з їхньої існування, тобто. на наявність файлів заданим шляхом. При виявленні невідповідності передбачені такі варіанти реакції на ситуації порушення цілісності:

- реєстрація події у журналі Secret Net;
- блокування комп'ютера;
- відновлення пошкодженої/модифікованої інформації;
- відхилення чи прийняття змін.

Самоконтроль підсистем СКЗІ проводиться перед входом користувача в систему і призначений для забезпечення гарантії того, що на момент завершення

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

завантаження ОС всі ключові компоненти Secret Net 12 завантажені та функціонують.

Система Secret Net 12 реєструє всі події, що відбуваються на комп'ютері: включення\вимкнення комп'ютера, вхід\вихід користувачів, події НСД, запуск додатків, звернення до конфіденційної інформації, контроль виведення конфіденційної інформації на друк та носії, що відчужуються.

В організації необхідно використовувати міжмережевий екран, який розділяє сегменти, мережі в яких обробляється конфіденційна інформація, персональні дані співробітників, а також інформація відкритого характеру.

Міжмережевий екран - комплекс апаратних або програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI відповідно до заданих правил. Для вирішення цього завдання підійде програмно-апаратний міжмережевий екран Cisco ASA 5505, який відповідає вимогам до 3-го класу захищеності відповідно до керівного документа «Засоби обчислювальної техніки. Міжмережеві екрани. Захист від несанкціонованого доступу до інформації. Показники захисту від несанкціонованого доступу до інформації»

Міжмережевий екран Cisco Systems серії ASA (Adaptive Security Appliances) - вископродуктивні пристрої для фільтрації трафіку, захисту від вірусів, хробаків та різних видів інтернет-атак, охорони периметра корпоративних мереж, організації шифрованих каналів через інтернет для зв'язку офісу та філій, а також для віддаленого підключення працівників та організації intranet-доступу.

Cisco ASA 5505 – багатофункціональний пристрій захисту ресурсів мережі від внутрішніх та зовнішніх атак. В інфраструктурі підприємства ASA 5505 займає місце класичного міжмережевого екрану (firewall), що дозволяє захистити мережу підприємства або окремі сегменти, але функціонал цього рішення набагато ширший.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

ASA 5505 поєднує в собі безліч технологій та рішень щодо забезпечення інформаційної безпеки.

Контроль з'єднань між вузлами мережі забезпечує вбудований міжмережевий екран з механізмами інспекції пакетів з урахуванням стану протоколу (stateful inspection firewall) на рівнях 2-7, який дозволяє стежити за станом усіх мережних комунікацій та допомагає запобігти несанкціонованому доступу до мережі. Механізми аналізу протоколів на прикладному рівні дозволяють забезпечити захист від нелегального використання дозволених портів, наприклад HTTP – TCP порт 80 для ICQ та інших додатків.

ASA 5505 може функціонувати в «безшумному» режимі, при цьому вона не буде видимим вузлом мережі, прозоро для користувача пропускатиме трафік, забезпечуючи необхідний рівень захисту.

ASA 5505 реалізує частину функцій сучасного маршрутизатора, такі як протоколи динамічної маршрутизації RIP та OSPF, резервування каналів доступу до мережі Інтернет, механізми забезпечення якості обслуговування (QoS).

Для забезпечення можливості відновлення всіх критично важливих даних та програм після виходу з ладу автоматизованої робочої станції, сервера або псування цифрового носія інформації, необхідно мати належні засоби резервного копіювання.

Резервне копіювання – процес створення копії даних на цифровому носії, призначеної для відновлення даних в оригінальному місці їх розташування у разі пошкодження або руйнування.

Для вирішення завдання резервного копіювання рекомендується використовувати програмний продукт Drive Backup 10 Workstation, який необхідно встановити на кожну робочу станцію, де планується резервне копіювання даних. Для віддаленого адміністрування програми можна встановити на будь-якому комп'ютері, що входить до складу локальної обчислювальної мережі підприємства Paragon Remote Manager 2.0.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

Для зберігання резервних копій використовується сервер у сегменті мережі з відкритою інформацією, в інші сегменти додані комп'ютери, на ці комп'ютери також пропонується встановити засоби захисту інформації несанкціонованого доступу, а також консоль віддаленого адміністрування Paragon Remote Manager 2.0.

Від комп'ютерів, призначених для зберігання резервних копій, не вимагається високої продуктивності, основна вимога - відносно великий обсяг дискового простору. Рекомендується використовувати ПК з об'ємом дискового простору більше 1 ТБ.

Адміністратор безпеки налаштовує розклад завдань резервного копіювання кожної машини за допомогою консолі управління, або створює розклад завдань для окремих робочих груп. Керування контрольними точками резервування та дисковим простором, виділеним під резервні копії, відбувається автоматично.

Адміністратор безпеки повинен регулярно переглядати звіти завдань, які формуються віддаленими клієнтами, та слідкувати за станом резервних архівів.

3.17 Висновки до розділу 3

В третьому розділі дипломної роботи було проведено проектування, розміщення та реалізація комп'ютерної мережі підприємства. Було проведено підбір необхідного активного та пасивного обладнання, здійснено налаштування серверного сегменту комп'ютерної мережі. Також було проведено проектування політики безпеки та доступу до ресурсів мережі підприємства. В кінці розділу було показано схему реалізації комп'ютерної мережі підприємства та проведено її тестування.

Впровадження системи інформаційної безпеки (СІБ) виявиться ефективною, якщо вона надійно підтримуватиме виконання правил політики безпеки.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Етапи побудови політики безпеки – це внесення до опису об'єкта автоматизації структури цінності та проведення аналізу ризику, а також визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають певний рівень цінності.

Правові заходи забезпечення безпеки комерційної таємниці є першочерговими, т. я. вони мають забезпечити ефективне функціонування інших заходів забезпечення конфіденційності інформації. З цього погляду правові заходи є первинними стосовно інших заходів.

Усі документи мають пройти погодження з юридичною службою підприємства, затверджено керівництвом та введено в дію наказом по підприємству. При цьому необхідно також враховувати, що документи повинні відповідати законам та іншим правовим документам України у цій галузі, оскільки на працівників накладаються певні обмеження та відповідальність, аж до кримінальної, за порушення правил роботи з комерційною таємницею.

На підприємстві пропонується запровадити програмний комплекс QBE_Systems. Використання системи QBE_Systems дозволяє комплексно вирішити всі завдання, пов'язані з керуванням доступом та обліковими даними користувачів. При цьому роль QBE_Systems полягає у формуванні та узгодженні заявок на доступ, а також реалізації та контролю доступу. Саме це завдання є ключовими для комплексного управління доступом.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

ВИСНОВКИ

Інформаційна безпека виявиться ефективною, якщо вона надійно підтримувати виконання правил політики безпеки. Етапи побудови політики безпеки – це внесення до опису об'єкта автоматизації структури цінності та проведення аналізу ризику, а також визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають певний рівень цінності.

Правові заходи забезпечення безпеки комерційної таємниці є першочерговими, т. я. вони мають забезпечити ефективне функціонування інших заходів забезпечення конфіденційності інформації. З цього погляду правові заходи є первинними стосовно інших заходів.

За результатами аналізу об'єкта захисту та огляду технічних засобів можна розробити проект модернізації існуючої інформаційної системи. Модернізована система забезпечує надійний захист об'єкта від несанкціонованого проникнення та повністю відповідає вимогам компанії у сфері ІТ-безпеки. При виборі технічних засобів особлива увага приділялася їх функціональним характеристикам та технічній сумісності пристроїв. Представлений концепт-модель системи повністю відповідає вимогам для компанії «GoodBud» та готовий бути одним з основних компонентів найбільш стабільної та безпечної обробки інформації в процесі роботи компанії.

У дипломній роботі було проведено проектування, розміщення та реалізація комп'ютерної мережі підприємства. Було проведено підбір необхідного активного та пасивного обладнання, здійснено налаштування серверного сегменту комп'ютерної мережі. Також було проведено проектування політики безпеки та доступу до ресурсів мережі підприємства.

На підприємстві пропонується запровадити програмний комплекс QBE_Systems. Використання системи QBE_Systems дозволяє комплексно вирі-

		Литвинюк В.С.			KIK.KP.B – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		98

шити всі завдання, пов'язані з керуванням доступом та обліковими даними користувачів. При цьому роль QBE_Systems полягає у формуванні та узгодженні заявок на доступ, а також реалізації та контролю доступу. Саме це завдання є ключовими для комплексного управління доступом.

Таким чином, у даній роботі було запропоновано заходи щодо захисту інформації, які дозволять уникнути ризиків та втрат. Розроблена система вжиття заходів щодо забезпечення інформаційної безпеки виправдає себе через 5 років.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : зб. наук. пр. Київ : Вид.- поліграф. центр «Київ. ун-т», 2019. – 256 с.

2. Закон України "Про інформацію" // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651.

3. Закон України "Про державну таємницю" // ВВР. – 1994. – № 16. – Ст. 93. Вводиться в дію Постановою ВР № 3856-XII від 21.01.94, ВВР, 1994, № 16, ст.94. Із змінами, внесеними згідно із Законами № 1169-VII від 27.03.2014.

4. Закон України "Про електронні документи та електронний документообіг" //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст.349.

5. Закон України "Про електронний цифровий підпис" // ВВР. – 2003. – № 36. – Ст. 276. Із змінами, внесеними згідно із Законами № 879-VI від 15.01.2009, ВВР, 2009, № 24, ст.296 // № 5284-VI від 18.09.2012.

6. Закон "Про Національну програму інформатизації" // ВВР. – 1998. - № 27-28. - ст.181. Із змінами, внесеними згідно із Законами № 2684-III від 13.09.2001, ВВР, 2002, № 1, ст.3.

7. Закон "Про захист персональних даних" // ВВР. – 2010. - № 34. - ст. 481. Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564.

8. Закон "Про захист інформації в інформаційно-телекомунікаційних системах" // ВВР. – 1994. - №31 - ст.286. Із змінами, внесеними згідно із Законами N 879-VI (879-17) від 15.01.2009, ВВР, 2009, № 24, ст.296.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Указ президента України " Про Положення про порядок здійснення криптографічного захисту інформації в Україні" // 22.05.1998, Л. Кучма № 505/98. Із змінами, внесеними згідно з Указами Президента // № 1019/98 (1019/98) від 15.09.98 // № 1229/99 (1229/99) від 27.09.99 // № 333/2008 (333/2008) від 11.04.2008 // № 693/2009 (693/2009) від 28.08.2009.

10. Конституція України. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. - Режим доступу: <http://portal.rada.gov.ua/>.

11. Максимов Н.В. Технические средства информатизации/Н.В. Максимов, М.: Форум, 2013 – 608 с.

12. Ярочкин В.И. Информационная безопасность: учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2009. – 216 с.

13. Домарев В. В. Безопасность информационных технологий. Системный подход - К.: ООО ТИД Диа Софт, 2004. - 992 с.

14. Поляк-Брагинский А.В. Локальная сеть. Самое необходимое/А.В. Поляк-Брагинский, Спб.: БВХ-Петербург, 2011 – 576.

15. Кавун С. В. Інформаційна безпека : навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : Вид. ХНЕУ, 2008. – 352 с.

16. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий/В.А. Сердюк, М.: Высшая Школа Экономики (Государственный Университет), 2013 – 576 с.

17. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал «Безпека інформації». — 2014. — № 1. — С. 7–11.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Петросян Р.В.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

18. Шевченко А. С. Модель загроз для відомчих безпроводових інформаційно-комунікаційних систем в умовах інформаційної боротьби при впливі комплексу навмисних атак порушника / А. С. Шевченко // Сучасний захист інформації. — 2011. — № 3. — С. 58–65.

19. Гундарь К.Ю. , Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах - К:"Корнійчук" 2000. – 256 с.

20. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510 с.

21. Скотт Бармен. Разработка правил информационной безопасности. - К: Вильямс.2002. – 300 с.

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Литвинюк В.С.			КІК.КР.Б – 123 – 16 – ПЗ	Арк.
		Пертросян Р.В.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема бази даних проекту

