Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Хіблін Миколи Миколайовича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування засобів захисту інформації комп'ютерної мережі ТОВ «ЯВІР ДНІПРО-1»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Хібліну Миколи Миколайовичу* **академічної групи** *125-19ск-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Обґрунтування засобів захисту інформації комп'ютерної мережі ТОВ «ЯВІР ДНІПРО-1»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 №268-с

Розділ	Зміст	Термін виконання
Розділ 1	Виконати класифікацію загроз безпеки інформації, навести заходи забезпечення безпеки комп'ютерної мережі підприємства	29.03.2022
Розділ 2	Розробка комплексної системи захисту інформації комп'ютерної мережі товариства з обмеженою відповідальністю «ЯВІР ДНІПРО-1»	24.05.2022
Розділ 3	Виконати розрахунок економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі	14.06.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2022р.

Дата подання до екзаменаційної комісії: 15.06.2022р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 109 с., 11 рис., 9 табл., 7 додатків, 23 джерел.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1»ммм від несанкціонованого доступу.

У розділі Стан питання. У постановці задачі описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У спеціальному розділі описана кратка характеристика об’єкту інформаційної діяльності ТОВ «ЯВІР ДНІПРО-1», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

В економічному розділі наведені розрахунки й обґрунтовані всі заходи щодо вдосконалення системи захисту інформації в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1».

Практичне значення роботи полягає в підвищенні рівня інформаційної безпеки мережі шляхом програмних, апаратних і організаційних заходів.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, МІЖМЕРЕЖЕВИЙ ЕКРАН, СИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК, ПАРОЛЬНИЙ ЗАХИСТ.

РЕФЕРАТ

Пояснительная записка: 109 стр., 11 рис., 9 табл., 7 приложений, 23 источника литературы.

Цель работы: с помощью программных, аппаратных и организационных мер улучшить защищенность информации в компьютерной сети ООО «ЯВИР ДНЕПР-1» от несанкционированного доступа.

В разделе Состояние вопроса. В постановке задачи описаны наиболее распространенные угрозы безопасности и основные положения защиты информации от них.

В специальном разделе описана краткая характеристика объекта информационной деятельности ООО «ЯВИР ДНЕПР-1», разработаны и описаны методы повышения защиты от несанкционированного доступа.

В экономическом разделе приведены расчеты и обоснованы все меры по усовершенствованию системы защиты информации в компьютерной сети ООО «ЯВИР ДНЕПР-1».

Практическое значение работы состоит в повышении уровня информационной безопасности сети, путём программных, аппаратных и организационных мероприятий.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, МЕЖСЕТЕВОЙ ЭКРАН, СИСТЕМА ОБЪЯВЛЕНИЯ И ПРЕДУПРЕЖДЕНИЯ АТАК, ПАРОЛЬНАЯ ЗАЩИТА.

ABSTRACT

Explanatory note: 109 p., 11 fig., 9 tab., 7 additions, 23 sources.

Purpose: To improve the security of information on the computer network of LLC «YAVIR DNEPR-1»

against unauthorized access through software, hardware and organizational measures.

In the Question status section. The problem statement describes the most common security threats and the basic provisions for protecting information from them.

The special section describes a brief description of the object of information activity of LLC «YAVIR DNEPR-1», developed and describes methods to improve the protection of information from unauthorized access.

The economic section presents the calculations and substantiated all measures to improve the information security system in the computer network of LLC «YAVIR DNEPR-1».

The practical value of the thesis is to increase the level of information security of the network through software, hardware and organizational activities.

INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY, THREAT MODEL, VIOLATOR MODEL, FIREWALL, ATTACK DETECTION AND PREVENTION SYSTEM, PASSWORD PROTECTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВВС - взаємодія відкритих систем;

ІзОД - інформація з обмеженим доступом;

ІС - інформаційна система;

КЗ - контрольована зона;

КМ - комп'ютерна мережа;

НД ТЗІ - нормативний документ технічного захисту інформації;

ОІД - об'єктом інформаційної діяльності;

ОС - операційна система;

ПЕМВ - побічні електромагнітні випромінювання;

ПЗ - програмне забезпечення;

ПК - персональний комп'ютер;

СОВ - система виявлення вторгнень;

СУБД - Система управління базами даних;

CSMA - Carrier Sense Multiple Access, мережевий протокол канального рівня;

FTP - File Transfer Protocol, протокол передачі файлів через мережу;

HIPS - Host-based Intrusion Prevention System, система запобігання вторгненням;

IP - internet protocol, протокол мережевої адресації;

ISO - International Organization for Standardization, міжнародний стандарт;

IT - Information technology, інформаційні технології;

OSI - Open Systems Interconnection, еталонна модель;

PGP - Pretty Good Privacy, система захисту;

SET - Secure Electronic Transaction, протокол;

SFT - System Fault Tolerance, система стійкості до відмов;

S/MIME - Secure/Multipurpose Internet Mail Extensions, система захисту стандарту мережі Інтернет;

WWW - World Wide Web, всесвітня павутина.

ЗМІСТ

ВСТУП

В даний час дуже широко використовується термін «комп'ютерна безпека». За останній час відсоток використання комп'ютерних мереж, а особливо Інтернету значно виріс, тому сьогодні термін «комп'ютерна безпека» використовується для опису проблем, пов'язаних з мережевим використанням комп'ютерів і їх ресурсів.

Сучасні інформаційні технології потребують організації високого рівня захисту даних. Комп'ютерна безпека має велике значення для забезпечення захищення систем обробки та зберігання даних. Об'єктами комп'ютерної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури.

Особливості захисту персональних комп'ютерів (ПК) обумовлені специфікою їх використання. Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації. Стандартність архітектурних принципів побудови, обладнання та програмного забезпечення персональних комп'ютерів, висока мобільність програмного забезпечення і ряд інших ознак визначають порівняно легкий доступ професіонала до інформації, що знаходиться в ПК

Винахід комп'ютера і подальший бурхливий розвиток інформаційних технологій в другій половині XX століття зробили проблему захисту інформації настільки актуальною і гострою, наскільки актуальна сьогодні інформатизація для всього суспільства.

У бізнесі, добросовісна конкуренція припускає суперництво, засноване на дотриманні законодавства і загальновизнаних норм моралі. Проте нерідко підприємці, конкуруючи між собою, прагнуть за допомогою протиправних

дій отримати інформацію в збиток інтересам іншої сторони і використовувати її для досягнення переваги на ринку. Криміналізація суспільства і недостатня ефективність державної системи охорони правопорядку примушує представників бізнесу самим приймати заходи для адекватного протистояння негативним процесам, що мають місце, завдають збитку конфіденційної інформації фірми.

В Україні, як і в інших державах світу, невпинно розвиваються нові галузі економіки, що ґрунтуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема Інтернету.

Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину.

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

- перехід від традиційної «паперової» технології зберігання і передачі відомостей на електронну і недостатній при цьому розвиток технології захисту інформації в таких технологіях;

- об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

- збільшення складності програмних засобів.

Отже головна тенденція, що характеризує розвиток сучасних інформаційних технологій, - зростання числа комп'ютерних злочинів і пов'язаних з ними розкрадань конфіденційної і іншої інформації, а також матеріальних втрат.

У роботі вирішуються проблеми несанкціонованого доступу до інформації через комп'ютерну мережу підприємства або мережу Internet.

ТОВ «ЯВІР ДНІПРО-1» на даному етапі свого існування, прагне до розширення і економічного зростання. З цього виходить, що в даний час необхідно побудувати ефективну систему захисту комп'ютерної мережі.

У проекті передбачається підвищення безпечної роботи комп'ютерної мережі, поліпшення умов праці і економічне обґрунтування комплексів заходів захисту інформації в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Класифікація загрози безпеці та пошкодження даних у комп'ютерних мережах

Із часом до Інтернету під'єднується дедалі більше користувачів. Зараз будь-яка людина може отримати доступ до даних, що зберігаються в Інтернеті, або створити свій власний вебресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, ускладнюючи їх виявлення й покарання. Зловмисники розміщують шкідливі програми на вебресурсах, «маскують» їх під корисне й безкоштовне програмне забезпечення. Тому важливо запобігти небезпеці, уникнути можливих загроз.

Під загрозою розуміють будь-які обставини та події, що виникають у зовнішньому середовищі, які у відповідних умовах можуть викликати появу небезпечної події.

Інформаційна загроза - це потенційна можливість певним чином порушити інформаційну безпеку.

Під інформаційною безпекою розуміють захищеність даних та інфраструктури, що її підтримує, від будь-яких випадкових або зловмисних дій, результатом яких може стати нанесення шкоди безпосередньо даним, їхнім власникам або інфраструктурі, що підтримує інформаційну безпеку.

Стандартною моделлю безпеки даних може слугувати модель із трьох категорій:

Конфіденційність - стан даних, за якого доступ до них здійснюють тільки ті особи, що мають на нього право.

Цілісність - уникнення несанкціонованої зміни даних та існування даних у неспотвореному вигляді.

Доступність - уникнення тимчасового або постійного приховування даних від користувачів, котрі мають права доступу.

Відповідно до розглянутої моделі безпеки даних є три різновиди загроз:

1. Загроза порушення конфіденційності полягає в тому, що дані стають відомими тому, хто не має права доступу до них. Вона виникає щоразу, коли отримано доступ до деяких секретних даних, що зберігаються в комп'ютерній системі чи передаються від однієї системи до іншої. Іноді, у зв'язку із загрозою порушення конфіденційності, використовується термін «витік даних».

2. Загроза порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу. Вона виникає, коли зловмисники навмисно змінюють дані, тобто порушується їхня цілісність.

Цілісність даних також може бути порушена внаслідок випадкової помилки програмного або апаратного забезпечення.

Санкціонованими змінами є ті, які зроблені уповноваженими особами з обґрунтованою метою (наприклад, санкціонованою зміною є періодична запланована корекція деякої бази даних).

3. Загроза відмови служб (загроза доступності) виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп'ютерної системи. Блокування буває постійним, якщо доступ до запитуваного ресурсу ніколи не буде отримано, або воно може викликати тільки затримку запитуваного ресурсу, досить довгу для того, щоб він став непотрібним. У цих випадках говорять, що ресурс вичерпано.

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій.

До категорії дій, що здійснюються авторизованими користувачами, належать: цілеспрямована крадіжка або знищення даних на робочій станції чи сервері; пошкодження даних користувачами в результаті необережних дій.

Другу категорію загроз становлять електронні методи впливу, які здійснюють хакери.

Хакер - кваліфікований ІТ-фахівець, який знається на комп'ютерних системах і втручається в роботу комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері.

Їхні мотиви можуть бути різними: помста, самовираження (дехто робить це задля розваги, інші - щоб показати свою кваліфікацію), винагорода. Останнім часом поняття «хакер» використовується для визначення мережевих зломщиків, розробників комп'ютерних вірусів й інших кіберзлочинців. У багатьох країнах злом комп'ютерних систем, розкрадання інформаційних даних, створення та поширення комп'ютерних вірусів і шкідливого програмного забезпечення переслідується законодавством.

Окрема категорія електронних методів впливу - комп'ютерні віруси та інші шкідливі програми. Вони становлять реальну небезпеку, широко використовуючи комп'ютерні мережі, Інтернет й електронну пошту. Дуже поширеною загрозою на сьогодні є спам.

Спам - небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.

Під загрозою безпеки інформації в комп'ютерній мережі (КМ) розуміють подію або дію, яка може викликати зміну функціонування КМ, пов'язану з порушенням захищеності оброблюваної в ній інформації.

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

Атакою на КМ називають дію порушником, що робиться, яке полягає в пошуку і використанні тієї або іншої уразливості. Інакше кажучи, атака на КМ є реалізація загрози безпеці інформації в ній.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

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

Уразливими є буквально всі основні структурно-функціональні елементи КМ: робочі станції, сервери, між мережеві мости (шлюзи, центри комутації), канали зв'язку і так далі.

Під загрозою в широкому розумінні зазвичай розуміють потенційно можливу подію, дію (вплив), процес або явище, які можуть призвести до нанесення збитку будь-якій зі сторін. Загрозою інтересам суб'єктів інформаційних відносин називають потенційно можливу подію, процес або явище, яке за допомогою дії на інформацію або інші компоненти інформаційної системи може прямо чи опосередковано призвести до завдання збитку.

У процесі зберігання і обробки інформація може піддатися діям чинників випадковим або умисним. Найчастішими і найнебезпечнішими, з огляду на розмір збитків, є ненавмисні помилки користувачів, операторів, системних адміністраторів й інших осіб, що обслуговують інформаційні системи, а також помилки, що виникають при обробці і передачі інформації. Згідно зі статистикою 65% втрат - наслідок ненавмисних помилок. Найрадикальніший спосіб боротьби з ненавмисними помилками - максимальна автоматизація і суворий контроль за правильністю виконуваних дій.

Загрози збоку навколишнього середовища відрізняються великою різноманітністю. В першу чергу це порушення інфраструктури - аварії в системі електроживлення, тимчасова відсутність зв'язку, перебої з водопостачанням, цивільні безлади та ін. Особливу небезпеку становлять стихійні лиха: пожежі, повені, землетруси, урагани. За даними статистики на ці загрози доводиться 13% втрат, завданих інформаційним системам. На рис. 1.1 проілюстровано в загальному вигляді класифікацію загроз інформації.

Штучні загрози - це загрози КМ, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

- ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проєктуванні КМ і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу тощо;

- навмисні (умисні) загрози, пов'язані з корисливими устремліннями людей (зловмисників).

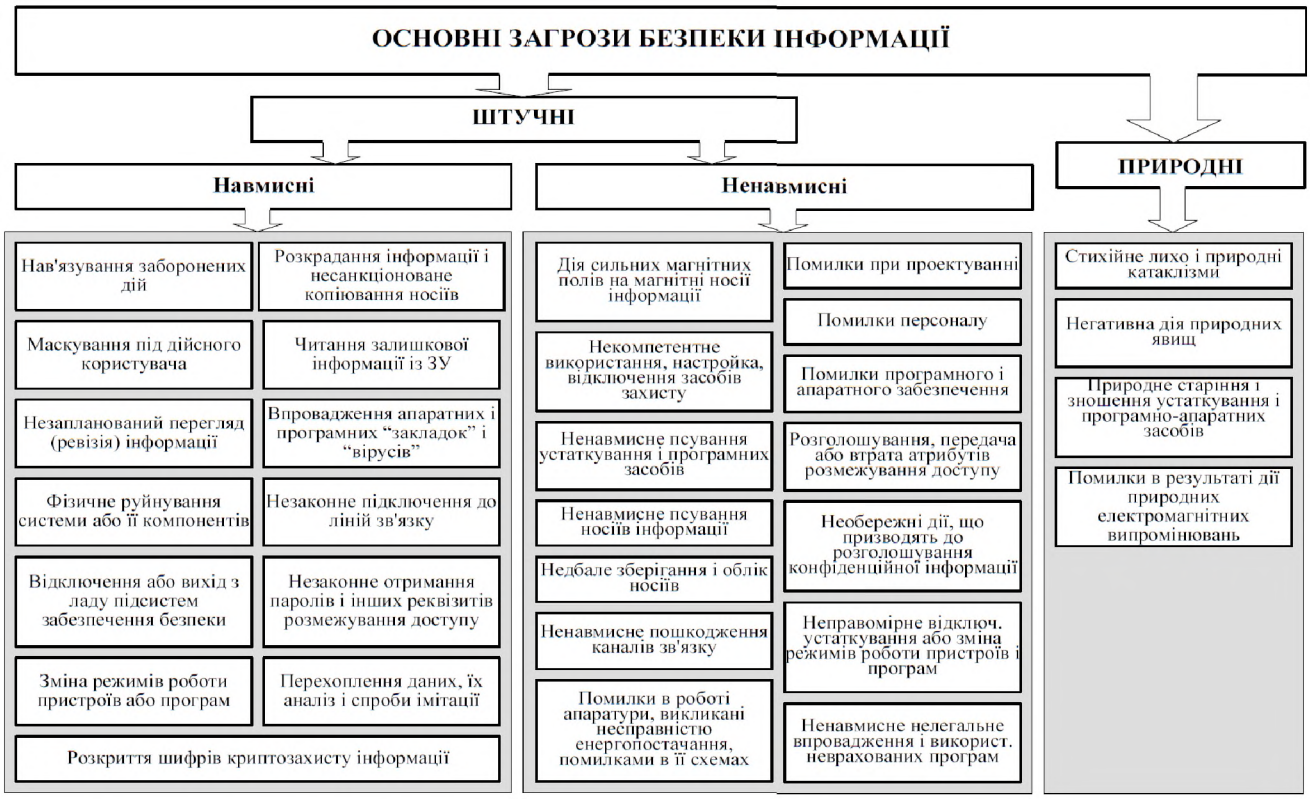


Рисунок 1.1 - Основні загрози безпеки інформації

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

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

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, сприяючих їх прояву і методів реалізації. І тоді ланцюжок зростає в схему, представлену на рисунку 1.2.

Загрози класифікуються по можливості нанесення збитку суб'єктові стосунків при порушенні цілей безпеки. Збиток може бути причинний яким-небудь суб'єктом (злочин, провина або недбалість), а також стати слідством, не залежним від суб'єкта проявів. Загроз не так вже і багато.

При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації і засобів її обробки, а також її втрата (ненавмисна втрата, витік). При забезпеченні цілісності інформації список загроз такий: модифікація (спотворення) інформації; заперечення достовірності інформації; нав'язування помилковій інформації. При забезпеченні доступності інформації можливе її блокування, або знищення самої інформації і засобів її обробки.

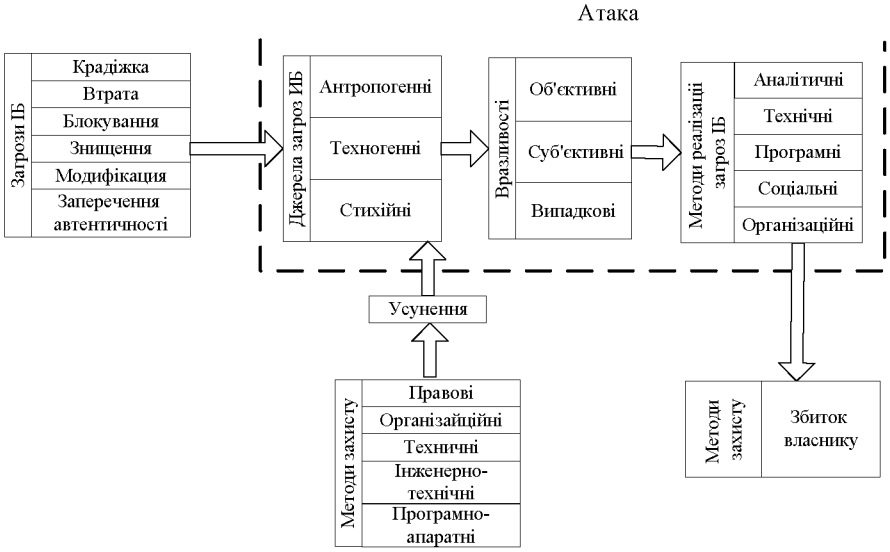


Рисунок 1.2 - Модель реалізації загроз інформаційній безпеці

На інформаційну безпеку організації можуть впливати різноманітні зовнішні чинники - «природні» загрози: причиною втрати даних може стати неправильне зберігання, крадіжка комп’ютерів і носіїв, форс-мажорні обставини тощо.

Таким чином, у сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоздатності й навіть життєздатності будь-якої організації.

1.2 Нормативно-правова база та міжнародні стандарти в галузі інформаційної безпеки КМ

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи

нормативно-правового регулювання відносин у цій сфері протидії загрозам цих інтересів та впорядкування відповідного правотворчого процесу.

Так, нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод здійснюється Конституцією України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про поштовий зв'язок» та ін. Вказані нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, спрямовані на реалізацію положень Доктрини безпеки особистості, держави і суспільства та ін.

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

- визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

- створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Необхідно визнати, що на сьогоднішній день проблема захисту інформації не має остаточного вирішення. Тому цей документ відображає сучасний стан проблеми і підходів до її розв'язання.

Міжнародна організація зі стандартизації (англ. International Organization for Standardization, ISO) - міжнародна організація, метою діяльності якої є ратифікація розроблених спільними зусиллями делегатів від різних країн стандартів.

Основні цілі розробки:

- уніфікація національних стандартів у сфері оцінки безпеки ІТ;

- підвищення рівня довіри до оцінки безпеки ІТ;

- скорочення витрат на оцінку безпеки ІТ на основі взаємного визнання сертифікатів;

Під загальним найменуванням «Інформаційна технологія. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій» складається з наступних частин:

- Частина 1. Вступ та загальна модель;

- Частина 2. Функціональні вимоги безпеки;

- Частина 3. Вимоги довіри до безпеки.

Якщо мають на увазі всі три частини стандарту, використовують позначення ISO/IEC 15408:2005.

Серед базових понять, що визначені в стандарті ISO/IEC 15408 слід виділити наступні:

- Задачі захисту (Security Objectives).

- Профіль захисту (Protection Profile).

- Завдання з безпеки (Security Target).

Поняття задач захисту визначає потребу споживачів продукту ІТ:

- у протистоянні заданій множині загроз безпеці;

- у необхідності реалізації політики безпеки.

Профіль захисту - це спеціальний нормативний документ, що містить:

- задачі захисту;

- функціональні вимоги;

- вимоги адекватності;

- їхнє обґрунтування, і служить керівництвом для розробника при створенні завдання з безпеки.

Завдання з безпеки - це спеціальний нормативний документ, що містить:

- задачі захисту;

- функціональні вимоги;

- вимоги адекватності;

- загальні специфікації засобів захисту;

- їхнє обґрунтування,

та у ході кваліфікаційного аналізу служить як опис продукту ІТ.

1.3 Послуги і механізми захисту інформації

Перш ніж визначати засоби захисту інформації і будувати відповідну систему, необхідно проаналізувати основні послуги й механізми захисту інформації. Для цього розглянемо еталонну модель взаємодії відкритих систем (OSI) і класифікацію можливих атак на кожний з рівнів цієї моделі.

Еталонну модель OSI (англ. Open Systems Interconnection) було розроблену інститутом стандартизації ISO з метою розмежування функцій різних протоколів у процесі передачі інформації від одного абонента іншому. Подібних класів функцій було виділено 7. Вони одержали назву рівнів. Кожен рівень виконує певні завдання в процесі передачі блоку інформації, причому відповідний рівень на приймальній стороні проводить перетворення, зворотні тим, які проводив той же рівень на передавальній стороні. В цілому проходження блоку даних від відправника до одержувача показане на рис. 1.3.

Кожен рівень додає до пакета невеликий обсяг своєї службової інформації - префікс (на рисунку вони зображені як P1...P7). Деякі рівні в конкретній реалізації цілком можуть бути відсутніми. Дана модель дозволяє провести класифікацію мережевих атак відповідно до рівня їх дії.

Фізичний рівень відповідає за перетворення електронних сигналів у сигнали середовища передачі інформації (імпульси напруги, радіохвилі, інфрачервоні сигнали). На цьому рівні основним класом атак є "відмова в сервісі". Постановка шумів по всій смузі пропускання каналу може призвести до розриву зв'язку.

Канальний рівень керує синхронізацією двох і більшої кількості мережевих адаптерів, підключених до єдиного середовища передачі даних. Прикладом його є протокол Ethernet. Дії на цьому рівні також полягають в основному в атаці "відмова в сервісі". Проте, на відміну від попереднього рівня, тут проводиться перебій синхропосилань або самої передачі даних

періодичною передачею "без дозволу або передачею не в свій час". Мережевий рівень відповідає за систему унікальних імен і доставку пакетів за цим іменем, тобто за маршрутизацію пакетів. Відповідно й атаки на цьому рівні найчастіше спрямовані на конфіденційність і цілісність службової інформації, пов'язаної з адресацією і наявністю унікальних імен.

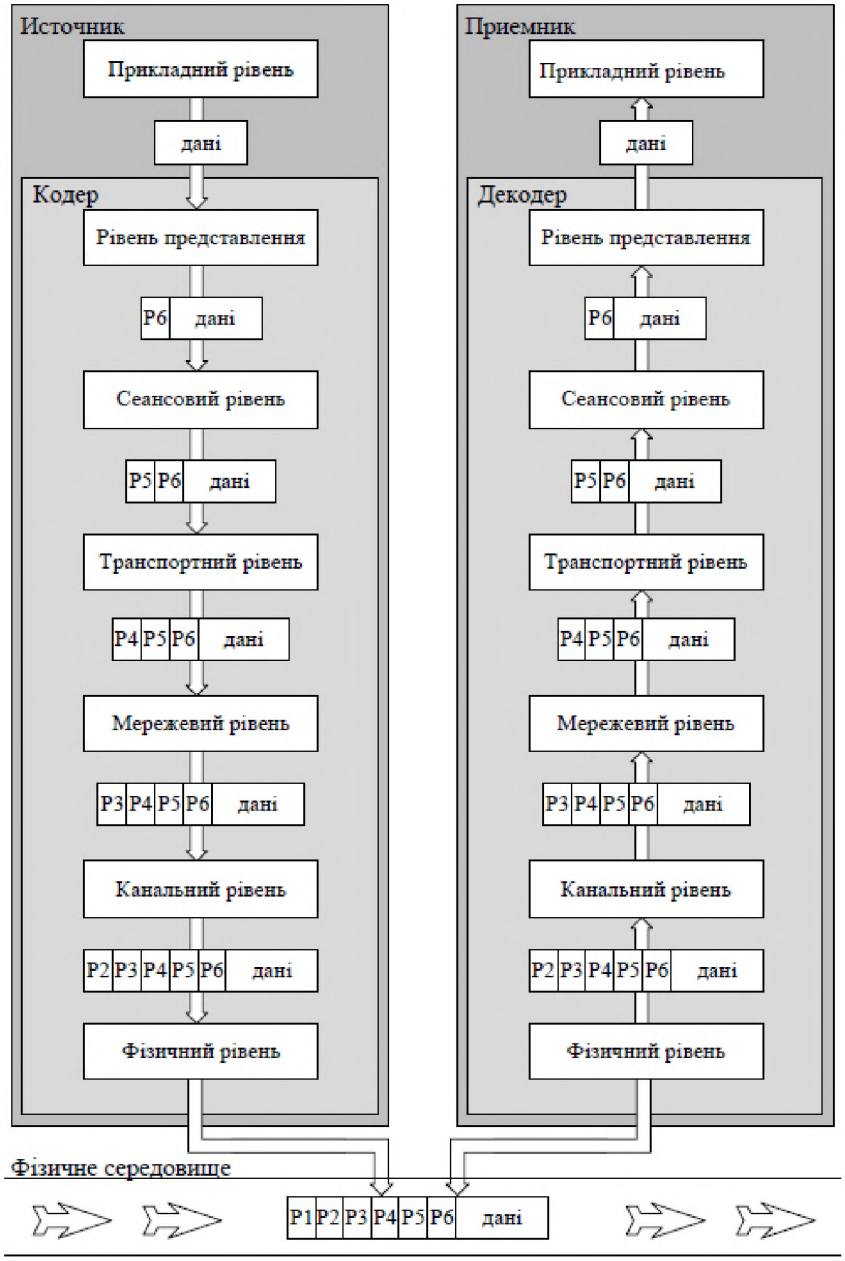


Рисунок 1.3 - Проходження блоку даних від відправника до одержувача відповідно до моделі взаємодії відкритих систем

Транспортний рівень відповідає за доставку великих повідомлень по лініях з комутацією пакетів. Оскільки в подібних лініях розмір пакета є

зазвичай невеликим числом (від 500 байт до 5 кілобайт), то для передачі великих обсягів інформації їх необхідно розбивати на передавальній стороні й збирати на приймальній. Вся річ у тому, що пакети на приймальну сторону можуть приходити й іноді приходять не в тому порядку, в якому вони були відправлені. Причина зазвичай полягає у втраті деяких пакетів через помилки або переповненість каналів, рідше - у використанні для передачі потоку двох альтернативних шляхів у мережі.

Отже, операційна система повинна зберігати деякий буфер пакетів, чекаючи приходу тих, що затрималися в процесі передачі. А якщо зловмисник з наміром формує пакети так, щоб послідовність була великою і свідомо неповною, то тут можна чекати як постійної зайнятості буфера, так і небезпечних помилок через його переповнення.

Сеансовий рівень відповідає за процедуру встановлення початку сеансу і підтвердження (квитування) приходу кожного пакета від відправника одержувачу. У мережі Інтернет протоколом сеансового рівня є протокол TCP (він займає і 4-й, і 5-й рівні моделі OSI). Відносно сеансового рівня дуже поширена специфічна атака класу «відмова в сервісі», основана на властивостях процедури встановлення з'єднання в протоколі TCP. Вона одержала назву SYN-Flood (flood - англ. «великий потік»).

Представницький рівень визначає формат, використаний для обміну даними між мережевими комп'ютерами і відповідає за перетворення протоколів, трансляцію даних, їх шифрування, зміну або перетворення вжитого набору символів (кодової таблиці) і розширення графічних команд. Представницький рівень, крім того, керує стисненням даних для зменшення переданих бітів. У зв'язку з цим особливо небезпечними є атаки, що спрямовані на спотворення даних (порушення цілісності), які часто призводять до зупинки в роботі окремих вузлів у комп'ютерних мережах.

Прикладний рівень - найвищій рівень моделі OSI. Він є вікном для доступу прикладних процесів до мережевих послуг. Цей рівень забезпечує послуги, що безпосередньо підтримують додатки користувача, такі, як

програмне забезпечення для передачі файлів, доступу до баз даних, електронна пошта. Прикладний рівень керує загальним доступом до мережі і обробкою помилок. Широко використовуваним розподіленим додатком на цьому рівні є електронна пошта. У зв'язку з цим спостерігається інтерес до засобів забезпечення автентифікації і конфіденційності оброблюваних даних.

Методологічною основою розробки системи захисту інформації є стандарт ISO/IEC 15408, згідно з яким основними нормативними документами, що характеризують інформаційну систему з точки зору безпеки, є профіль захисту (protection profile) і проєкт забезпечення безпеки (security target). Під профілем захисту розуміють незалежну множину функціональних вимог безпеки і вимог адекватності, спрямованих на задоволення потреб споживача. Проєктом безпеки є безліч вимог безпеки й специфікацій функцій безпеки.

Відповідно до основних положень міжнародних стандартів життєвий цикл системи захисту інформації складається з п'яти етапів:

1. Визначення політики безпеки, яка містить абстрактний ряд вимог до безпеки системи.

2. Аналіз вимог безпеки, включаючи аналіз ризиків, аналіз урядових, правових і стандартних вимог.

3. Визначення послуг безпеки, необхідних для задоволення поставлених вимог.

4. Побудова і впровадження системи безпеки, включаючи вибір механізмів безпеки, що забезпечують конкретні вибрані послуги безпеки.

5. Безперервне управління безпекою.

Послуга безпеки призначена для забезпечення захисту від ідентифікованої загрози. Існують абстрактні поняття, які можуть бути використані для характеристики вимог безпеки. Механізмом безпеки є засіб, за допомогою якого реалізується і застосовується відповідна послуга.

Стандарти ISO 7498, ISO/IEC 10181 визначають п'ять базових загальноприйнятих послуг безпеки (рис. 1.4).

Під конфіденційністю розуміють властивість системи, яка гарантує, що

інформація не може бути доступна або розкрита для неавторизованих (неуповноважених) осіб, об'єктів або процесів.

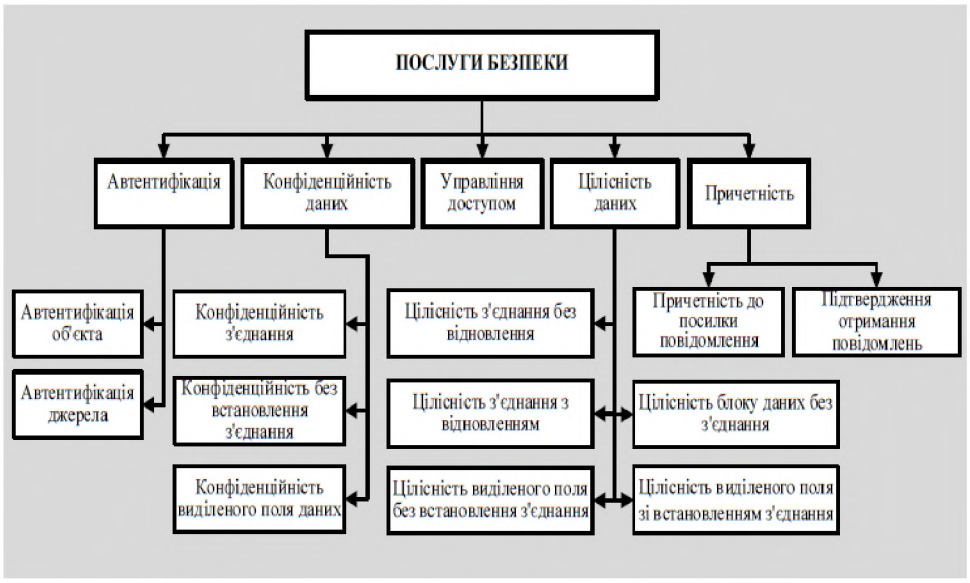


Рисунок 1.4 - Загальна класифікація послуг безпеки

Цілісність даних - послуга, що гарантує можливість модифікації тієї інформації, яка міститься в комп'ютерній системі і зв'язку, й пересилається по каналах, тільки суб'єктами, які мають на це право.

Під причетністю розуміють здатність запобігання можливості відмови одним з реальних учасників комунікацій від факту його повної або часткової участі в передачі даних.

Доступність визначається як додаткова послуга забезпечення захищеності інформаційних систем. Механізми забезпечення доступності запобігають атакам, що мають на меті унеможливити доступ до ресурсів або послуг інформаційної системи (або зробити їх "якість" незадовільною) для користувача. На рис. 1.5 подано розподіл послуг безпеки по рівнях моделі взаємодії відкритих систем (ВВС). Як видно з наведеного рисунка, велика частина послуг безпеки доводиться на верхні рівні моделі ВВС, переважно, на

рівень прикладного процесу. Розглянемо основні системи і протоколи, що забезпечують захист інформації на різних рівнях моделі ВВС.

На прикладному рівні в теперішній час для забезпечення захисту інформації найчастіше використовуються дві системи - PGP і S/MIME.

PGP (англ. Pretty Good Privacy) - широко розповсюджена система захисту, незалежна від будь-якої організації або органу влади. Тому вона підходить як для індивідуального користування, так і для включення в конфігурацію мережі будь-якої організації. S/MIME (англ. Secure / Multipurpose Internet Mail Extensions) є системою захисту, спеціально розробленою як стандарт мережі Інтернет.

Зростання популярності Word Wide Web (WWW) для електронної комерції і розповсюдження інформації привело до виникнення гострої необхідності в забезпеченні захисту відповідних даних у Web. Забезпечити виконання ряду послуг дозволяє застосування протоколів SSL/TLS і SET. Протокол призначений для забезпечення надійного захисту наскрізної передачі даних з використанням протоколу TCP. Протокол SET - це відкриті специфікації шифрування і захисту, розроблені з метою захисту транзакцій, що виконуються в мережі Інтернет за допомогою пластикових платіжних карток.

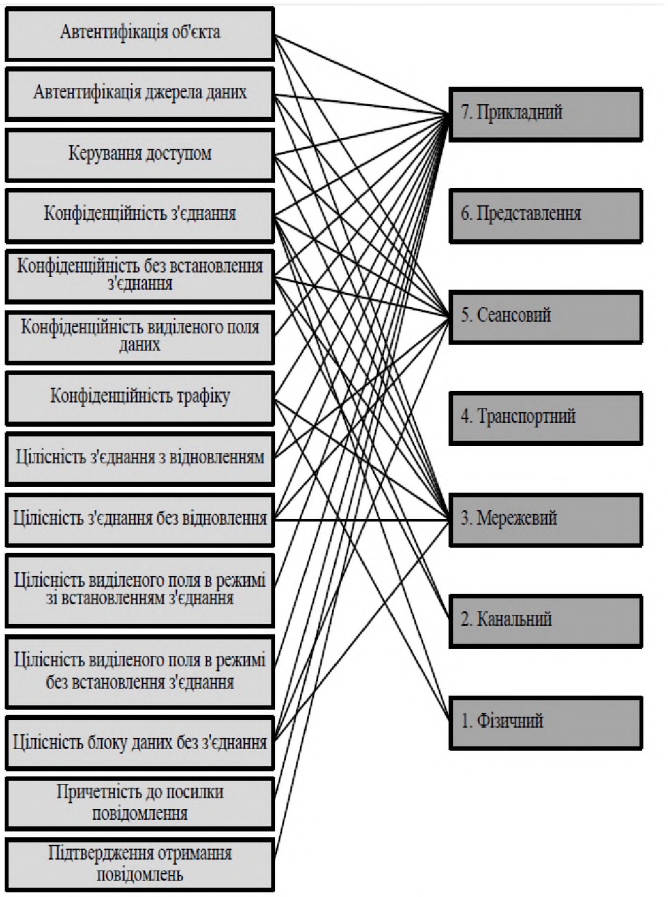


Рисунок 1.5 - Розподіл послуг безпеки по рівнях еталонної моделі ВВС

Незважаючи на розробку цілого ряду механізмів захисту на прикладному і сеансовому рівні, існує необхідність забезпечення безпеки на мережевому рівні. Наприклад, підприємство може захистити свою мережу TCP/IP за допомогою заборони доступу до ненадійних вузлів, шифруючи пакети даних, що передаються з мережі підприємства, і вимагаючи автентифікації пакетів, що входять у цю мережу із зовні. За допомогою реалізації захисту на мережевому рівні організація може забезпечити роботу в мережі не тільки додатків, які мають свої засоби захисту, але і додатків, що не володіють такими засобами. Захист на рівні IP (мережевому) охоплює 3 сфери безпеки: автентифікацію, конфіденційність, керування ключами.

Механізми безпеки є конкретними заходами для реалізації послуг безпеки. Взаємозв'язок послуг і механізмів безпеки подано на рис. 1.6.

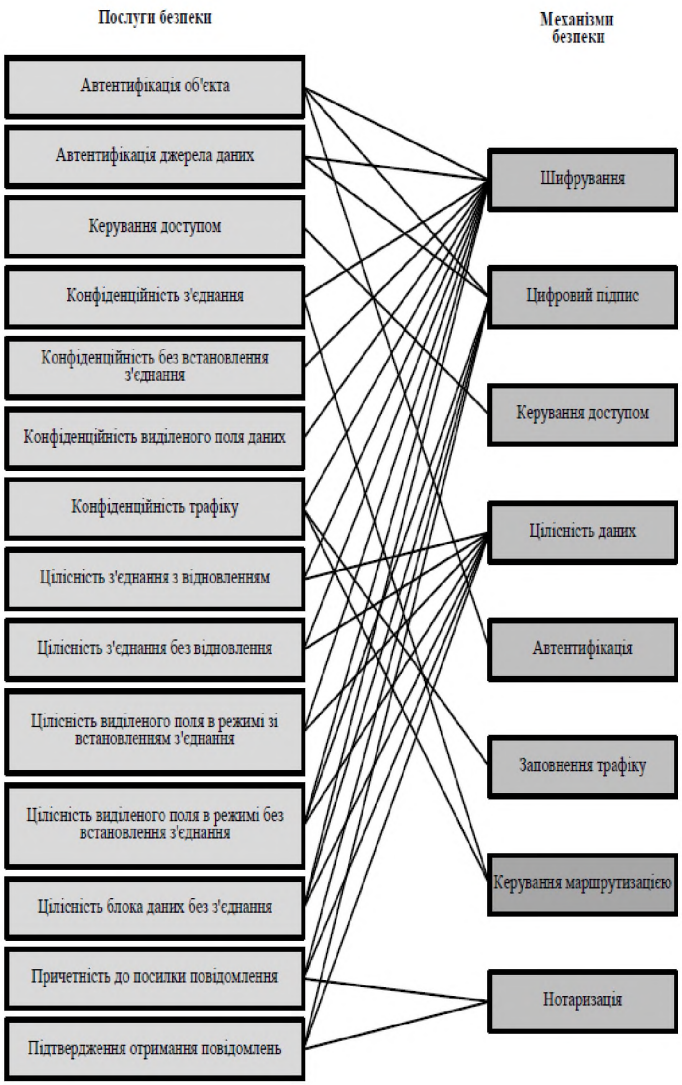


Рисунок 1.6 - Взаємозв'язок послуг і механізмів безпеки

Стандарт поділяє механізми безпеки на два класи, а саме: спеціальні механізми забезпечення безпеки, які використовуються для реалізації специфічних послуг і різняться для різних послуг, та загальні механізми, які не належать до конкретних послуг безпеки.

До спеціальних механізмів забезпечення безпеки належать такі:

- шифрування (encipherment);

- механізми цифрового підпису (digital signature mechanisms);

- механізми управління доступом (access control mechanisms);

- механізми забезпечення захисту цілісності даних (data integrity mechanisms), які включають криптографічні контрольні функції;

- механізми автентифікації (authentication exchange mechanisms);

- механізми заповнення трафіку (padding traffic mechanisms);

- механізми керування маршрутизацією (routing control mechanisms).

Механізми шифрування припускають використання криптографічних перетворень даних для того, щоб зробити їх нечитабельними або неосмисленими. Шифрування застосовується спільно зі зворотною функцією - розшифрування.

Цифровий підпис є цифровим еквівалентом підпису (друку, штампа та ін.), наявність якого в повідомленні дозволяє з високою точністю визначити джерело повідомлення (документа) і юридично довести, що, з певною ймовірністю, тільки він міг створити і підписати цей документ.

Механізми керування доступом використовуються для забезпечення послуг керування доступом і реалізують політику керування доступом.

При ухваленні рішень про надання запрошуваного типу доступу можуть використовуватися такі види й джерела інформації:

- бази даних керування доступом, в яких можуть знаходитися списки керування доступом або структури аналогічного призначення;

- паролі або інша ідентифікаційна інформація;

- ідентифікаційні документи або інші посвідчення, пред'явлення яких свідчить про наявність прав доступу;

- позначки безпеки, асоційовані з суб'єктами й об'єктами доступу;

- час запрошуваного доступу;

- маршрут запрошуваного доступу;

- тривалість запитуваного доступу й інша інформація.

- механізми нотаризації (notarisation mechanisms).

Механізми цілісності даних діляться на два типи механізмів:

- механізми захисту цілісності окремого пакета даних;

- механізми захисту цілісності послідовності пакетів даних.

Автентифікація джерела даних часто забезпечується шляхом використання механізму захисту цілісності даних спільно з шифруванням або цифрового підпису. Логічна автентифікація користувача комп’ютерної системи здійснюється на основі пароля.

Автентифікація об'єкта комунікації зазвичай виконується за допомогою подвійного або потрійного підтвердження з'єднання або «рукостискання» аналогічно процедурі синхронізації пакетів у протоколах зі встановленням з'єднання.

Механізм заповнення трафіку застосовується для забезпечення конфіденційності трафіку. Заповнення трафіку може включати генерацію випадкового трафіку, заповнення додатковою інформацією інформативних пакетів, передачу пакетів через проміжні станції в «непотрібному» напрямі. Обидва типи пакетів, як інформативний, так і випадковий, можуть доповнюватися до постійної довжини.

Механізми нотаризації привертають третю сторону, що користується довірою двох суб'єктів, для забезпечення підтвердження комунікаційних характеристик переданих даних. Такими комунікаційними характеристиками є цілісність, час, особи відправників і одержувачів. Найчастіше механізми нотаризації застосовуються для забезпечення послуги підтвердження причетності. Для підтвердження причетності відправника даних нотаризація застосовується спільно з цифровим підписом на основі «відкритого» ключа.

Нотаризація може також застосовуватися для забезпечення надійної тимчасової позначки, що забезпечується «тимчасовим нотаріусом».

Така позначка може містити підпис «нотаріуса», ідентифікатор повідомлення, імена відправника і одержувача, а також зареєстровані час і дату отримання повідомлення. При цьому «нотаріус» не має доступу до самого повідомлення, що забезпечує конфіденційність повідомлення.

Механізми керування маршрутизацією застосовуються для забезпечення конфіденційності з метою запобігання контролю за шляхом проходження даних від відправника до одержувача. Вибір шляху може здійснюватися або крайовою системою, реалізуючи маршрутизацію, яка

Довірча функціональність використовується разом з іншими механізмами безпеки і є сукупністю рекомендацій і способів, які повинні реалізовуватися для забезпечення гарантії правильної і надійної роботи інших механізмів

безпеки. Довірча функціональність припускає широке використання нормативної документації при розробленні програмних або апаратних засобів, що реалізовують механізми безпеки.

Механізми виявлення подій в системах захисту інформації служать для виявлення як спроб порушення безпеки, так і для реєстрації легітимної активності користувачів. Виявлення може бути локальним або дистанційним і реалізуватися через тривожну сигналізацію про події (event reporting (alarm)), реєстрацію подій (event logging) і відновлювальної дії (recovery actions).

Під контролем безпеки розуміють незалежний розгляд і аналіз записів безпеки з метою перевірки достатності керування системою, гарантувати відповідність функціонування системи політиці безпеки і рекомендувати необхідні зміни в управлінні, політиці і процесах безпеки. Зазвичай розглядають дві процедури: протоколювання і аудит. Під протоколюванням розуміють збирання і накопичення інформації про події, що відбуваються в інформаційній системі. Під аудитом розуміють оперативний аналіз накопиченої інформації, що проводиться постійно або періодично.

Механізми відновлення безпеки виконують функцію реакції системи на порушення безпеки. Такими діями можуть бути, наприклад, негайне роз'єднання або припинення роботи, відмова суб’єкту в доступі, тимчасове позбавлення суб'єкта прав, занесення суб'єкта в «чорний список» та ін.

1.4 Основні загрози інформаційної безпеки комп’ютерних систем і мереж

Однією з важливих проблем безпеки мережевого середовища є зловмисні або, принаймні, небажані спроби вторгнення в мережу, що виконуються деякими користувачами або програмним забезпеченням. Такого роду порушення з боку користувачів можуть мати форму спроб несанкціонованого доступу до комп’ютера або спроб легального користувача одержати привілеї або виконати операції, які виходять за рамки наданих йому повноважень. Під порушеннями з боку програмного забезпечення мають на увазі роботу вірусу, «черв’яка» або «троянського коня».

Усі ці порушення належать до питань захисту мереж, оскільки вхід до системи може здійснюватися за допомогою мережі. Проте ці порушення не можна віднести до чисто мережевих. Користувач, що має доступ до локального терміналу, може спробувати проникнути до системи, не використовуючи мережевих засобів. Вірус або «троянський кінь» можуть потрапити до системи з дискети. У цьому сенсі тільки «черв'як» може вважатися чисто мережевим засобом вторгнення в систему. Таким чином, питання вторгнення до системи знаходяться на перетині галузей, що належать до захисту мереж і захисту комп'ютерних систем.

Однією з двох найпоширеніших загроз безпеки є порушники (другою загрозою є віруси), яких називають хакерами (hacker) або зломщиками (cracker). Дамо класифікацію порушників.

- Імітатор (masquerader) - це особа, що не має права користуватися комп'ютером, але подолала механізм керування доступом і використовує права доступу деякого легального користувача.

- Правопорушник (misfeasor) - це легальний користувач, що намагається дістати доступ до даних, програм або ресурсів, до яких він не має відповідних прав доступу, або користувач, який має в своєму розпорядженні відповідні права доступу, але використовує їх в зловмисних цілях.

- Таємний користувач (clandestine user) - це особа, що заволоділа правами керування системою і використовує ці права для обходу засобів аудиту і керування доступом або для створення перешкод у реєстрації системних подій.

За метою впливу розрізняють три основні типи загроз безпеці інформаційних систем:

- загрози порушення конфіденційності інформації;

- загрози порушення цілісності інформації;

- загрози порушення працездатності системи (відмови в обслуговуванні).

Порушення конфіденційності та цілісності інформації, а також доступності і цілісності певних ресурсів ІС можуть бути викликані різними небезпечними впливами на інформаційну систему. Сучасні автоматизовані

системи обробки інформації представляють собою складну систему, що складається з великої кількості компонент різного ступеня автономності, які зв'язані між собою та обмінюються даними. Практично кожний компонент може піддаватися зовнішньому впливу чи вийти з ладу. Компоненти інформаційної системи можна розділити на такі групи:

- апаратні засоби;
- програмне забезпечення;
- дані;
- персонал

Небезпечні впливи на ІС можна поділити на випадкові та зловмисні. Аналіз досвіду проєктування, виготовлення та експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах функціонування інформаційної системи. Причинами випадкових впливів можуть бути:

- аварійні ситуації, пов'язані зі стихійними лихами та відключеннями електричного живлення;
- відмови та збоїв апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу та користувачів;
- завади в лініях зв'язку, спричинені впливом зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Порушником може бути співробітник, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути зумовлені різними мотивами: невдоволенням співробітника своєю кар'єрою, матеріальною зацікавленістю, цікавістю, конкурентною боротьбою, прагненням самоствердження та ін. Виходячи з можливості виникнення найнебезпечнішої ситуації, зумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;

- порушнику відома інформація про принципи роботи системи;

Можна виділити такі приклади навмисних загроз:

- несанкціонований доступ сторонніх осіб, що не належать до числа співробітників, та ознайомлення з конфіденційною інформацією;

- ознайомлення співробітників з інформацією, до якої вони не повинні мати доступ;

- несанкціоноване копіювання програм і даних;

- викрадення носіїв інформації, що містять конфіденційну інформацію;

- викрадення роздрукованих документів;

- навмисне знищення інформації;

- несанкціонована модифікація співробітниками фінансових документів, звітності та баз даних;

- фальсифікація повідомлень, що передаються по каналах зв'язку;

- відмова від авторства повідомлення, переданого каналом зв'язку;

- відмова від факту отримання інформації;

- пошкодження інформації, викликане впливом вірусів;

- пошкодження архівної інформації, розміщеної на змінних носіях;

- викрадення обладнання.

Несанкціонований доступ є найбільш розповсюдженим та різностороннім видом комп'ютерних порушень. Суть несанкціонованого доступу полягає в отриманні користувачем (порушником) доступу до об'єкту з порушенням правил розмежування доступу, встановлених у відповідності до прийнятої в організації політики безпеки. Несанкціонований доступ використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, некоректному їх встановленні та настроюванні. Несанкціонований доступ може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Із всього розмаїття способів та прийомів несанкціонованого доступу зупинимося на найбільш розповсюджених та зв'язаних між собою порушеннях:

- перехоплення паролів;

- «маскарад»;

- незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача ввійти в систему програма-перехоплювач імітує на екрані введення логіну та паролю користувача, які пересилаються власнику програми-перехоплювача після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач вважає, що допустив помилку при введенні паролю. Він повторює введення і отримує доступ в систему. Власник програми-перехоплювача, отримавши логін та пароль законного власника, може тепер їх використовувати в своїх цілях. Існують й інші способи перехоплення паролів.

«Маскарад» - це виконання якихось дій одним користувачем від імені іншого, що має відповідні повноваження. Метою «маскараду» є приписування якихось дій іншому користувачу або присвоєння повноважень та привілеїв іншого користувача. Прикладами реалізації «маскараду» є:

- вхід в систему під іменем та паролем іншого користувача (такому «маскараду» передує перехоплення паролю);

- передача повідомлень в мережі від імені іншого користувача.

«Маскарад» є особливо небезпечним в банківських системах електронних платежів, де неправильна ідентифікація клієнта із-за «маскараду» зловмисника може привести до великих втрат законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожний користувач отримує свій набір привілеїв: звичайні користувачі - мінімальний, адміністратори - максимальний.

Окремо слід зупинитися на загрозах, яким можуть піддаватися комп'ютерні мережі. Основна особливість будь-якої комп'ютерної мережі полягає в тому, що її компоненти розподілені в просторі. При вторгненні в комп'ютерну мережу зловмисник може використовувати як пасивні, так і активні методи вторгнення. При пасивному вторгненні (перехопленні

інформації) порушник тільки спостерігає за проходженням інформації по каналу зв'язку, не втручаючись ні в інформаційний потік, ні в зміст інформації. Як правило, зловмисник може визначити пункти призначення та ідентифікатори або тільки факт проходження повідомлення, його довжину та частоту обміну, якщо зміст повідомлення розпізнати неможливо, - виконати аналіз трафіку (потоку повідомлень) в даному каналі.

При активному вторгненні порушник прагне підмінити інформацію, що передається в повідомленні. Він може вибірково модифікувати чи змінювати повідомлення, затримувати чи змінювати порядок слідування повідомлень. Зловмисник може також анулювати і затримувати усі повідомлення, що передаються по каналу. Такі дії можна кваліфікувати як відмову в передачі повідомлень.

Комп'ютерні мережі характерні тим, що крім звичайних локальних атак, які здійснюються в межах однієї системи, проти об'єктів мереж здійснюють так звані, віддалені атаки. Зловмисник може перебувати за тисячі кілометрів від атакованого об'єкта, при цьому нападу може піддаватися не тільки конкретний комп'ютер, а й інформація, що передаються по мережним каналам зв'язку. Під віддаленою атакою розуміють інформаційний зловмисний вплив на розподілену комп'ютерну мережу, який здійснюється програмно з використанням каналів зв'язку.

У табл. 1.1 показані основні шляхи реалізації загроз безпеці інформаційної системи (ІС) при впливі на її компоненти. Ця таблиця дає тільки загальну картину того, що може відбутися з системою, а конкретні обставини та особливості повинні розглядатися окремо.

Таблиця 1.1 - Шляхи реалізації загроз безпеці ІС

Об'єкти впливу	Порушення конфіденційності інформації	Порушення цілісності інформації	Порушення працездатності системи
Апаратні	Несанкціонований	Несанкціонований	Несанкціонований

засоби	доступ - підключення; використання ресурсів; викрадення носіїв	доступ - підключення; використання ресурсів; модифікація, зміна режимів	доступ - зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ - копіювання; викрадення; перехоплення	Несанкціонований доступ - впровадження «троянських коней», «вірусів», «черв'яків»	Несанкціонований доступ- спотворення; знищення; підміна
Дані	Несанкціонований доступ - копіювання; викрадення; перехоплення	Несанкціонований доступ - спотворення; модифікація	Несанкціонований доступ- спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	«Маскарад»; вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

1.5 Методи і технології захисту комп'ютерних мереж

Для вирішення проблеми захисту інформації, основними засобами, використовуваними для створення механізмів захисту, прийнято вважати:

1. Технічні засоби - електричні, електромеханічні, електронні і ін. типу пристрою. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Слабкі сторони - недостатня гнучкість, відносно великі обсяг і маса, висока вартість. Технічні засоби поділяються на:

- апаратні пристрої, що вбудовуються безпосередньо в апаратуру, або пристрої, що сполучаються з апаратурою локальних мереж по стандартному інтерфейсу (схеми контролю інформації з парності, схеми захисту полів пам'яті по ключу, спеціальні регістри);

- фізичні - реалізуються у вигляді автономних пристроїв та систем (електронно-механічне обладнання охоронної сигналізації та спостереження. Замки на дверях, грати на вікнах).

2. Програмні засоби

Програмні засоби - програми, спеціально призначені для виконання функцій, пов'язаних з захистом інформації. А саме програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку.

Недоліки - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

3. Змішані апаратно-програмні засоби

Змішані апаратно-програмні засоби, які реалізують ті ж функції, що й апаратні та програмні засоби окремо, і мають проміжні властивості.

4. Організаційні засоби

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації та розвитку. Недоліки - висока залежність від суб'єктивних чинників, у тому числі від спільної організації роботи в конкретному підрозділі.

У ході розвитку концепції захисту інформації фахівці прийшли до висновку, що використання якого-небудь з вище зазначених способів захисту, не забезпечує надійного збереження інформації. Необхідний комплексний підхід до використання та розвитку всіх засобів і способів захисту інформації.

1.5.2 Програмні засоби захисту інформації КМ

За ступенем поширення і доступності на першому місці стоять програмні засоби, тому далі вони розглядаються більш докладно. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

Серед програмних засобів захисту інформації в локальних мережах можна виділити і детальніше розглянути такі:

- засоби архівації даних - засоби, що здійснюють злиття декількох файлів і навіть каталогів в єдиний файл - архів, одночасно зі скороченням загального обсягу вихідних файлів шляхом усунення надмірності, але без втрат інформації, тобто, з можливістю точного відновлення вихідних файлів.;

- антивірусні програми - програми розроблені для захисту інформації від вірусів;

- криптографічні засоби включають способи забезпечення конфіденційності інформації, у тому числі за допомогою шифрування і аутентифікації;

- засоби ідентифікації і аутентифікації користувачів - аутентифікацією (встановлення достовірності) називається перевірка належності суб'єкта доступу пред'явленого ним ідентифікатора та підтвердження його достовірності. Іншими словами, аутентифікація полягає в перевірці: чи є суб'єкт, який підключається тим, за кого він себе видає. А ідентифікація забезпечує виконання функцій встановлення автентичності та визначення повноважень суб'єкта при його допуску в систему, контролювання встановлених повноважень в процесі сеансу роботи, реєстрації дій та ін.

- засоби керування доступом - засоби, що мають метою обмеження та реєстрацію входу-виходу об'єктів на заданій території через «точки проходу»;

- протоколювання і аудит - протоколювання забезпечує збір та накопичення інформації про події, що відбуваються в інформаційній системі.

Аудит - це процес аналізу накопиченої інформації. Метою комп'ютерного аудиту є контроль відповідності системи або мережі необхідним правилам безпеки, принципам або індустріальним стандартам. Аудит забезпечує аналіз

усього, що може ставитися до проблем безпеки, або все, що може призвести до проблем захисту.

1. Вбудовані

Вбудовані засоби захисту інформації в мережевих ОС доступні, але не завжди, як уже зазначалося, можуть повністю вирішити виникаючі на практиці проблеми. Наприклад, мережні ОС NetWare 3.x, 4.x дозволяють здійснити надійний «ешелонований захист" даних від апаратних збоїв та пошкоджень. Система SFT (System Fault Tolerance - система стійкості до відмов) компанії Novell включає три основні рівня:

SFT Level I передбачає, зокрема, створення додаткових копій FAT і Directory Entries Tables, негайну верифікацію кожного знову записаного на файловий сервер блоку даних, а також резервування на кожному жорсткому диску близько 2 % від обсягу диска. При виявленні збою дані перенаправляються в зарезервовану область диска, а збійний блок позначається як «поганий» і в подальшому не використовується.

SFT Level II містить додаткові можливості створення «дзеркальних дисків», а також дублювання дискових контролерів, джерел живлення й інтерфейсних кабелів.

SFT Level III дозволяє застосовувати в локальній мережі дубльовані сервери, один з яких є «головним», а другий, що містить копію всієї інформації, вступає в роботу в разі виходу головного сервера з ладу.

Система контролю та обмеження прав доступу в мережах NetWare (захист від несанкціонованого доступу) також містить кілька рівнів:

- рівень початкового доступу (включає ім'я та пароль користувача, систему облікових обмежень: таких як, явний дозвіл або заборону роботи, допустимий час роботи у мережі місце на жорсткому диску, займане особистими файлами даного користувача, і т. д.);

- рівень прав користувачів (обмеження на виконання окремих операцій та/або на роботу даного користувача, як члена підрозділу, в певних частинах файлової системи мережі);

- рівень атрибутів каталогів і файлів (обмеження на виконання окремих операцій, у тому числі видалення, редагування або створення, що йдуть з боку файлової системи і стосуються всіх користувачів, що намагаються працювати з даними каталогами або файлами);

- рівень консолі файл-сервера (блокування клавіатури файл-сервера на час відсутності мережевого адміністратора до введення ним спеціального пароля).

2. Спеціалізовані

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

- Firewalls - брандмауерів (firewall - вогняна стіна). Між локальною і глобальною мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь трафік мережевого рівнів, що проходить через них. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю.

Більш захищений різновид методу - це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік надсилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

- Proxy-сервери (proxy - довіреність, довірена особа).

Весь трафік мережевого/транспортного рівнів між локальною і глобальною мережами забороняється повністю - маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не

дає достатнього захисту проти атак на більш високих рівнях - наприклад, на рівні програми (віруси, код Java і JavaScript).

1.6 Аналіз захищеності КМ

Сервіс аналізу захищеності призначений для виявлення вразливих місць з метою їх оперативної ліквідації. Сам по собі цей сервіс ні від чого не захищає, але допомагає виявити (і усунути) пропуски в захисті раніше, ніж їх зможе використовувати зловмисник. Насамперед, маються на увазі не архітектурні (їх ліквідовувати складно), а «оперативні» проломи, що з'явилися в результаті помилок адміністрування або із-за неуваги до оновлення версій програмного забезпечення.

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

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

В принципі, можуть виявлятися проломи самої різної природи: наявність шкідливого ПЗ (зокрема, вірусів), слабкі паролі користувачів, невдало сконфігуровані операційні системи, небезпечні мережеві сервіси, невстановлені латки, уразливості в застосуваннях і так далі проте найбільш ефективними є мережеві сканери (очевидно, через домінування сімейства протоколів TCP/IP), а також антивірусні засоби. Антивірусний захист ми зараховуємо до засобів аналізу захищеності, не вважаючи за її окремий сервіс безпеки.

Сканери можуть виявляти вразливі місця як шляхом пасивного аналізу, тобто вивчення конфігураційних файлів, задіяних портів і тому подібне, так і шляхом імітації дій того, що атакує. Деякі знайдені вразливі місця можуть усуватися автоматично (наприклад, лікування заражених файлів), про інших повідомляється адміністраторові.

Контроль, що забезпечується системами аналізу захищеності, носить реактивний характер, що запізнюється, він не захищає від нових атак, проте слід пам'ятати, що оборона має бути ешелонованою, і як один з рубежів контролю захищеності цілком адекватний. Відомо, що переважну більшість атак носить рутинний характер; вони можливі тільки тому, що відомі проломи в захисті роками залишаються неусуненими.

1.7 Висновки

Сьогодні зміст категорії «захист інформації» все більше і більше пов'язується з безпечним функціонуванням автоматизованих (комп'ютерних) систем у всіх галузях суспільної діяльності. Досить актуальна проблема захисту інформації від різних загроз: - несанкціонований доступ - 2%; - укорінення вірусів - 3%; - технічні відмови апаратури мережі - 20%; - цілеспрямовані дії персоналу - 20%; - помилки персоналу (недостатній рівень кваліфікації) - 55%. Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові дії персоналу (людський фактор), оскільки вони становлять 75% усіх випадків.

Політика інформаційної безпеки, яку дійсно можна назвати хорошою і ефективною, повинна, перш за все, бути зрозуміла всім користувачам. Для вирішення цієї проблеми рекомендується проводити постійне ознайомлення користувачів з наявною політикою безпеки і не розцінювати такі дії як просту формальність. Користувачі повинні розуміти всю узяту на себе відповідальність і сприяти збереженню інформації. Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їх обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності. Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства.

У даному розділі проведений аналіз апаратних і програмних засобів захисту інформації загалом і в комп'ютерній мережі зокрема. Внаслідок чого були виявлені достоїнства і недоліки методів захисту інформації, їх можливості, а також можливості їх застосування.

Виконана постановка завдань, відповідно до яких головною метою даної роботи є підвищення ефективності заходів захисту інформації в комп'ютерній мережі. Отже, забезпечення інформаційної безпеки є актуальним завданням. Таким чином, сучасний розвиток інформаційних технологій, високий рівень комп'ютеризації й інформатизації сучасного суспільства зумовили виникнення нових загроз безпеки інформації. Швидке зростання обсягів оброблюваних даних у сучасних комп'ютерних системах і мережах, створення нових форм і способів обробки інформації, стрімкий розвиток обчислювальної техніки висувають підвищені вимоги до криптографічних засобів захисту інформації.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна характеристика підприємства

Об’єктом інформаційної діяльності (ОІД) є будівля в якій знаходиться товариство з обмеженою відповідальністю «ЯВІР ДНІПРО-1». Підприємство ТОВ «ЯВІР ДНІПРО-1» зареєстровано 30.01.2019 за юридичною адресою 49064, Дніпропетровська обл., місто Дніпро, проспект Сергія Нігояна, будинок 22/26 в п’яти поверховому будинку ОІД на першому поверсі.

Керівником організації є Афанасенко Олександр Анатолійович.

На момент останнього оновлення даних 01.05.2022 статус організації не перебуває в процесі припинення. Ситуаційний план представлений у додатку Б.

Область діяльності - охорона об’єктів (розробка, встановлення, налаштування, модернізація, обслуговування охоронних систем на об’єктах).

Організаційна структура ТОВ «ЯВІР ДНІПРО-1» зображена на рис. 2.1. Голова відділу технічного забезпечення має 2 бригади по 3 чоловіка на авто компанії, котрі виконують замовлення клієнтів.

Рисунок 2.1 Структурна схема управління ТОВ «ЯВІР ДНІПРО-1»

Співробітники які постійно знаходяться в головному офісу:

- Директор - 1 людина;
- Голова відділу технічного забезпечення - 1 людина;

- Головний менеджер - 1 людина;
- Головний бухгалтер - 1 людина;
- Бухгалтер - 1 людина;
- Спеціаліст з питань кібербезпеки - 1 людина;
- Системний адміністратор - 1 людина;
- Офіс менеджер - 1 людина.

Так само можна віднести до штату охоронців (2 людини) і прибиральницю (1 людина), які найняті всіма фірмами, що знаходяться в будівлі.

Режим роботи фірми:

Робочий день для співробітників підприємства починається з 9 до 18. Для прибиральниці робочий день з 8.30 до 9.00, окрім цього поверхневе прибирання приміщень і коридору під час обідньої перерви з 12.30 до 13.30. Системний адміністратор працює з 10:00 до 17:00.

2.2 Характеристика будівлі

Офіс приміщення ТОВ «ЯВІР ДНІПРО-1», де циркулює інформація з обмеженим доступом (ІзОД) розташований на першому поверсі 5-ти поверхового будинку з адміністративними приміщеннями. Генеральний план першого поверху ОІД представлений у додатку В.

Контрольована Зона (КЗ) - обмежена зовнішніми стінами будівлі, з інших боків внутрішніми стінами (коридором та іншими офісними приміщеннями). Під першим поверхом знаходяться підвал, зверху офіси адміністрації. Вхідні двері метал\мдф з 2-ома замками(циліндричними) під ключ та датчиком відкриття дверей.

Режим КЗ забезпечується таким чином:

Будівля має 5 поверхи та 3 окремих входи, перший поверх виділений під офіси співробітників тощо. На території є охоронець, який відповідає за доступ людей до приміщень. Відокремлений вхід зворотної сторони служить для входу жильців в будівлю. З головного входу можна потрапити тільки в приміщення

ТОВ «ЯВІР ДНІПРО-1». Охорона у будинку цілодобова, оскільки вони відповідають за будівлю.

Режим допуску до території будівлі забезпечується таким чином:

У робочий час вхід у приміщення допускається усьому персоналу після відкривання дверей директором або менеджером підприємства, які мають ключі від вхідних дверей офісу. Охорона спостерігає за безпекою та пересуванням відвідуючи за допомогою відеоспостереження.

Клієнти можуть заходити у офіс після обговорення часу зустрічі.

У не робочий час офіс ставиться під охорону централізованою системою сигналізації з 21:00 вечора до 9:00 ранку та двері зачиняють на 2 циліндричні замки під ключ. Охорона слідкує за допуском до будівлі лише за перепустками. Будівля має нічне відеоспостереження, освітлення, сигналізацію, датчики руху.

Вікна металопластикові, одностворчасті. На кожному вікні встановлені жалюзі.

ТОВ «ЯВІР ДНІПРО-1» має 10 кімнат, які займають площу 113 м^2:

- кімната№1 директора;
- кімната№2 менеджер 1;
- кімната№3 менеджер 2;
- кімната№4 головний менеджер;
- кімната№5 бухгалтер;
- кімната№6 голова відділу технічного забезпечення;
- кімната№7 головний бухгалтер;
- кімната№8 спеціаліста з питань кібербезпеки, системного адміністратора;
- кімната№9 приймальня офіс менеджера;
- кімната№10 серверна.

План поверху представлений у додатку Г.

Сусіди:

- 1 поверх: друга половина приміщення офіс;
- 2-5 поверхи: жильці;

- на півночі знаходяться чотири одноповерхових житлових будинків;

- на півдні знаходиться три чотирьох поверхових житлових будинків, два двох поверхових житлових будинків, два одноповерхових житлових будинків та трьох поверховий житловий будинок;

- на заході знаходиться одноповерховий житловий будинок;

- на сході знаходиться два одноповерхових житлових будинків, двох поверхових житловий будинок, трьох поверховий житловий будинок та п'ятиповерховий адміністративно житловий будинок.

2.3 Характеристика серверу і ПК

На підприємстві в серверній (кімната №10) встановлено джерело безперебійного живлення Eaton 9SX 6000i RT3U, та сервер ARTLINE Business T19 (T19v12) з харакристиками в таблиці 2.1.

Сервер використовується для резервного копіювання даних з ПК працівників або під час необхідності, який потім зберігається на сервері для подальшої обробки та роботи з ПЗ які потребуют обмеженого доступу.

Таблиця 2.1 - Характеристики обладнання серверної

Назва	Характеристики	
C1	Материнська плата	Intel B660
	Процессор	Intel Core i7-9700F (3.0 - 4.7 ГГц)
	ОЗУ 16 ГБ, DDR4-2933 МГц	64 ГБ DDR4-2666 МГц
	Відео карта	nVidia® GeForce® RTX 2060, 6144 МБ
	Блок живлення	850W
	Накопичувач	HDD: 2 x 1 ТБ, SSD: 2 x 250 ГБ
	Мережевий контроллер	Realtek RTL8111H
	RAID контроллер	0/1/5/10
K1	Комутатор	HP StorageWorks 8/8 SAN Switch AM867A 24-Port 8Gb FC 8 ports active
M1	Маршрутизатор	Tp-link Ultra (KN-1810)

У офісі для кожного співробітника встановлений окремий комп'ютер. Всі 10 комп'ютерів мають однакову характеристику монітор MSI 23.8" IPS

(1920x1080) Full HD та системний блок HP ProOne 440 G4 (4YV99ES) з харакристиками в таблиці 2.2:

Таблиця 2.2 - Характеристики робочих місць

Назва	Характеристики	
ПК1-ПК10	Материнська плата	Intel B460
	Процессор	Intel Core i5-9700F (3.0 - 4.7 ГГц)
	ОЗУ 16 ГБ, DDR4-2933 МГц	8 ГБ DDR4-2666 МГц
	Відео карта	nVidia® GeForce® RTX 2060, 6144 МБ
	Блок живлення	550W
	Накопичувач	SSD 500
	Мережевий контроллер	Realtek RTL8111H

2.4 Перелік головних ПЗ

Основні ПЗ встановленні на підприємстві:

- ОС Windows Server 2016 Standard Edition, встановлено на сервері С1;

- ОС Microsoft Windows 10 Pro SP1 64-bit Russian (визначаються функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та має Експертний висновок №1027 дійсний з 26.09.2019) встановлено на всіх офісних ПК;

- Microsoft Office 2016 Pro, встановлено на всіх офісних ПК і сервері С1;

- CRM система для обліку клієнтів, встановлена сервері С1;

- Бухгалтерія BAS1C (тільки на комп'ютерах бухгалтерів та сервері);

- Бухгалтерія МЕДОК (тільки на комп'ютерах бухгалтерів та сервері);

- Антивірус NOD32 корпоративна версія на 15 ПК, ліцензія на 1 рік.

2.5 Характеристика оброблюваної інформації в комп'ютерній мережі

Інформація, яка циркулює на об'єкті за способом доступу ділиться на:

- відкриту: інформація про підприємство, рід діяльності, кількість робочих місць і персоналу, заробітна плата співробітників, інформація про послуги, які надається фірма - вся інформація, яка не потребує захисту.

- інформацією з обмеженим доступом - важливе для підприємства, порушення цілісності або доступності яких може привести до морального або матеріального збитку: інформація про замовників і поставників, про проєкти і розробки, фінансові відомості, про устаткування, про засоби реалізації продукції.

Директор підприємства самостійно встановлює ступінь допуску до циркулюючої інформації. Найвищий гриф секретності інформації на підприємстві: конфіденційно.

Функціональні ПЗ і офісні пакети встановлюються на робочі станції тільки для підтвердження дозволу адміністратора сети.

Вся інформація друкарського, документованого, архівного вигляду, а також системні журнали, технічна, експлуатаційна і розпорядча документація, в не залежності від терміну зберігання знаходиться в сейфі в кабінеті директора.

На сервері зберігається вся інформація, яка є конфіденційною. Терміни зберігання даної інформації встановлює директор підприємства:

- інформація про співробітників - 2 роки;
- інформація про партнерів - 3 року;
- інформація про постачальників - 2 року;
- розробки, проєкти, - 3 року;
- бізнес-плани - 2 роки;
- інформація про клієнтів - 3 року.

Документація, яка включає конфіденційну інформацію, дублюється - створюються резервні копії. Архівація даних проводиться один раз на тиждень засобами ОС. Під час процесу архівації запису користувачів на сервер припиняються, а сервер відключається. Архівація даних виконується стандартними засобами ОС Windows - «Майстер архівації і оновлення», який створює копію необхідних даних на жорсткому диску. Архівації підлягають: стан системи, системні служби і всі диски, пов’язані з компонентами ОС.

2.6 Авторизація та доступ до ОС

Конфіденційна інформація зберігається на сервері. Сервер знаходиться в серверній. Доступ до інформації з правом повного контролю, на сервері, мають спеціаліст з питань кібербезпеки та директор. При вході в ОС на сервері, користувачі наділені правом обмеженого доступу до інформації, яка зберігається на сервері, використовують систему введення особливого облікового запису і пароля.

Вхід в систему через введення особливого облікового запису і паролю.

Пароль є послідовністю символів і спеціальних символів, довга яких обмежена мінімальним порогом в 8 символів і максимальним - 12 символів.

Кількість введення пароля обмежена 3 спробами. Між спробами невірного пароля є тимчасова затримка для зменшення кількості спроб злому системи захисту.

Кожен працівник зберігає пароль в місці малодоступному зловмисникові або запам'ятовує його.

На робочій станції вхід в систему здійснюється після введення особливого облікового запису і пароля.

2.7 Модель загроз

Всі джерела загроз безпеці інформації, циркулюючої в корпоративній мережі можна розділити на три основні групи:

1. Загрози, обумовлені діями суб’єкта (антропогенні загрози);
2. Загрози, обумовлені технічними засобами (техногенні загрози);
3. Загрози, обумовлені стихійними джерелами.

Перша група найбільш велика і представляє найбільший інтерес з погляду організації парирування цим загрозам, оскільки дії суб’єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Методи протидії цим загрозам керовані і безпосередньо залежать від волі організаторів захисту інформації.

Суб’єкти, дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішні:

- кримінальні структури;

- рецидивісти і потенційні злочинці;

- недобросовісні партнери;

- конкуренти;

так і внутрішні:

- персонал установи;

- персонал філій;

- обличчя з порушеною психікою;

- спеціально упроваджені агенти.

Дії суб'єктів можуть привести до ряду небажаних наслідків, серед яких стосовно корпоративної мережі, можна виділити наступні:

1. Крадіжка:

- технічних засобів (вінчестерів, ноутбуків, системних блоків);

- носіїв інформації (паперових, магнітних, оптичних і ін.);

- інформації (читання і несанкціоноване копіювання);

- засобів доступу (ключі, паролі, ключова документація і ін.).

2. Підміна (модифікація):

- операційних систем;

- систем управління базами даних;

- прикладних програм;

- інформації (даних), заперечення факту відправки повідомлень;

- паролів і правил доступу.

3. Знищення (руйнування):

- технічних засобів (вінчестерів, ноутбуків, системних блоків);

- носіїв інформації (паперових, магнітних, оптичних і ін.);

- програмного забезпечення (ОС, СУБД, прикладного ПЗ)

- інформації (файлів, даних)

- паролів і ключової інформації.

4. Порушення нормальної роботи (переривання):

- швидкості обробки інформації;

- пропускній спроможності каналів зв'язку;
- об'ємів вільної оперативної пам'яті;
- об'ємів вільного дискового простору;
- електроживлення технічних засобів.

5. Помилки:

- при інсталяції ПЗ, ОС, СУБД;
- при написанні прикладного ПЗ;
- при експлуатації ПЗ;
- при експлуатації технічних засобів.

6. Перехоплення інформації (несанкціонований)

- за рахунок ПЕМВ від технічних засобів;
- за рахунок наведень по лініях електроживлення;
- за рахунок наведень по сторонніх провідниках;
- по акустичному каналу від засобів виводу;
- по акустичному каналу при обговоренні питань;
- при підключенні до каналів передачі інформації;
- за рахунок порушення встановлених правил доступу (злом).

Друга група містить загрози менш прогнозована, безпосередньо залежна від властивостей техніка і тому що вимагають особливої уваги. Технічні засоби, що містять потенційні загрози безпеці інформації так само можуть бути: внутрішніми (неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; допоміжні засоби (охорона, сигналізації, телефонії); інші технічні засоби, вживані в установі;) і зовнішніми (засоби зв'язку; близько розташовані небезпечні виробництва; мережі інженерних комунікації (енерго-, водопостачання, каналізації)).

Наслідками застосування таких технічних засобів, що безпосередньо впливають на безпеку інформації можуть бути:

1. Порушення нормальної роботи:

- порушення працездатності системи обробки інформації;
- порушення працездатності зв'язку і телекомунікацій;

- старіння носіїв інформації і засобів її обробки;

- порушення встановлених правил доступу;

- електромагнітна дія на технічні засоби.

2. Знищення (руйнування):

- програмного забезпечення, ОС, СУБД;

- засобів обробки інформації (кидки напруги, протечки);

- приміщень;

- інформації (розмагнічування, радіація, протечки та ін.);

- персоналу.

3. Модифікація (зміна):

- програмного забезпечення. ОС, СУБД;

- інформації при передачі по каналах зв'язку і телекомунікаціям.

Третю групу складають загрози, які абсолютно не піддаються прогнозуванню і тому заходи їх парирування повинні застосовуватися завжди. Стихійні джерела, що становлять потенційні загрози інформаційній безпеці як правило є зовнішніми по відношенню до даного об'єкту і під ними розуміються раніше всього природні катаклізми:

- пожежі;

- землетруси;

- повені;

- урагани;

- інші форс-мажорні обставини;

- різні непередбачені обставини;

- нез'ясовні явища.

У таблиці 2.3 наведені най можливіші загрози від персоналу підприємства.

Природні і нез'ясовні явища так само впливають на інформаційну безпеку, небезпечні для всіх елементів корпоративної мережі і можуть привести до наступних наслідків:

1. Знищення (руйнування):

- технічних засобів обробки інформації;
- носіїв інформації;
- програмного забезпечення (ОС, СУБД, прикладного ПЗ);
- інформації (файлів, даних);

Таблиця 2.3 - Аналіз загроз

Можливі загрози інформації	Директор	Голова відділу технічного забезпечення	Системний адміністратор та спеціаліст кібербезпеки	Менеджери	Бухгалтери	Офіс менеджер
Природні явища	0,16	0, 16	0,12	0,12	0,128	0,1
Військові дії	0,6	0,6	0,2	0,7	0,7	0,7
Відмови інженерно-технічних засобів захисту інформації	0,64	0,64	0,80	0,52	0,52	0,52
Відмови в мережі енергозабезпечення	0,064	0,064	0,32	0,16	0,16	0,16
Відмови компонентів комп'ютерів	0,08	0,08	0,8	0,8	0,8	0,8
Технічних засобів	0,75	0,75	0,64	0,52	0,52	0,52
Носіїв інформації	0,80	0,80	0,64	0,64	0,64	0,64
Засобів доступу	0,75	0,75	0,80	0,64	0,64	0,64
Програмних засобів	0,24	0,24	0,8	0,8	0,8	0,8
Даних	0,24	0,24	0,8	0,64	0,64	0,64
Паролів і правил доступу	0,75	0,75	0,8	0,8	0,8	0,8
Носіїв інформації	0,75	0,75	0,64	0,52	0,52	0,64
Програмного забезпечення	0,8	0,8	0,8	0,8	0,8	0,8
Інформації	0,6	0,6	0,8	0,8	0,8	0,8
Паролів і ключової інформації	0,6	0,6	0,8	0,8	0,8	0,8
Пропускній спроможності каналів зв'язку	0,04	0,04	0,8	0,8	0,8	0,8
Об'ємів вільної оперативної пам'яті	0,128	0,128	0,64	0,64	0,64	0,64
Об'ємів вільного дискового простору	0,8	0,8	0,8	0,8	0,75	0,8
За рахунок ПЕМІ від технічних засобів	0,8	0,8	0,8	0,8	0,75	0,8
За рахунок наведень по лініях електроживлення	0,024	0,75	0,8	0,8	0,8	0,8
За рахунок наведень по сторонніх провідниках	0,024	0,75	0,8	0,8	0,8	0,8
При підключенні до каналів передачі інформації	0,64	0,64	0,8	0,48	0,48	0,8
За рахунок порушення встановлених	0,64	0,64	0,8	0,48	0,48	0,8

правил доступу (злом)						
Разом	10,92	12,21	16	14,86	14,77	15,6

- приміщень;

- персоналу.

2. Зникнення (пропажа):

- інформації в засобах обробки;

- інформації при передачі по телекомунікаційних каналах;

- носіїв інформації;

- персоналу.

На основі аналізу, що проводиться різними фахівцями в області комп'ютерних злочинів і спостереженнями, по частоті прояву загрози безпеці можна розставити так:

- крадіжка (копіювання) програмного забезпечення;

- підміна (несанкціоноване введення) інформації;

- знищення (руйнування) даних на носіях інформації;

- порушення нормальної роботи (переривання) в результаті вірусних атак;

- модифікація (зміна) даних на носіях інформації;

- перехоплення (несанкціоноване знімання) інформації;

- крадіжка (несанкціоноване копіювання) ресурсів;

- порушення нормальної роботи (перевантаження) каналів зв'язку;

2.8 Характеристика комп'ютерної мережі підприємства

На підприємстві існує своя локальна мережа, доступ до якої мають тільки працівники ТОВ «ЯВІР ДНІПРО-1». В більшості випадків є доступ лише до обмеженого числа тек цієї мережі, необхідних в ході трудової діяльності. Так само в мережі має вихід в Internet. Інформація про кожен вихід в мережу і Internet фіксується системним адміністратором.

Кількість робочих станцій в мережі - 10 (ПК1-ПК10), поодинці на кожного співробітника.

План приміщень, де розташовані робочі станції і сервер представлений у додатку Г.

Мережа, як це видно з рисунку 2.2, має топологію «зірка».

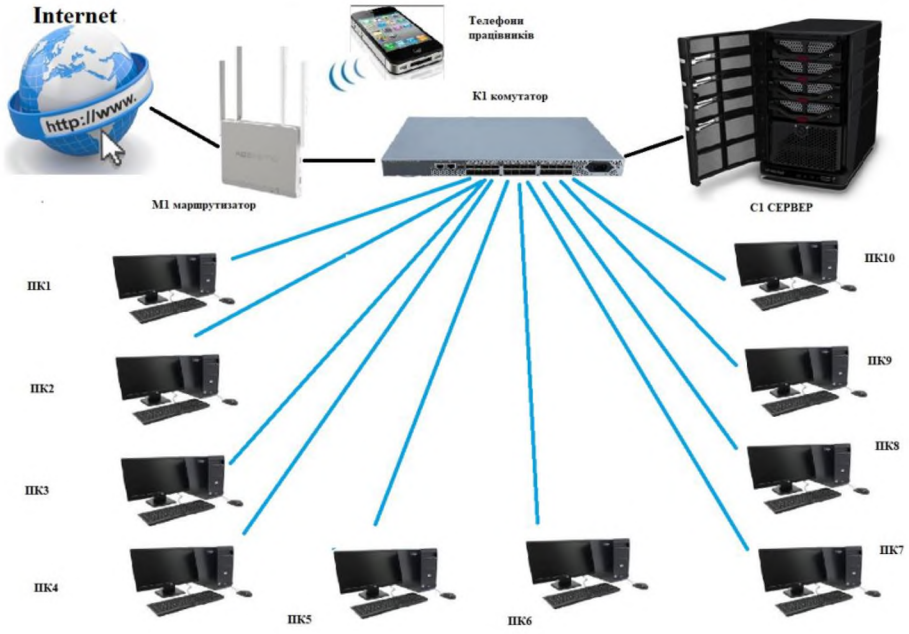


Рисунок 2.2 - Структура комп'ютерної мережі ТОВ «ЯВІР ДНІПРО-1».

Топологія типу «зірка» є продуктивнішою структурою, кожним комп'ютером, у тому числі і сервером, з'єднується окремим сегментом кабелю з центральним концентратором.

Основною перевагою такої мережі є її стійкість до збоїв, що виникають унаслідок неполадок на окремих ПК або із-за пошкодження мережевого кабелю.

Використовуваний метод доступу - CSMA/CD. Саме цей метод доступу застосовує мережева архітектура Ethernet, яка використовується на підприємстві.

Мережа побудована на основі на основі витої пари з використанням кабелю стандарту UTP (Unshielded Twisted Pair) неекранована витаючи пара, категорії 5е, міжнародного стандарту кабельних систем.

2.9 Характеристика серверної ОС

Windows Server - це платформа для створення інфраструктури підключених програм, мереж та вебсервісів. забезпечує безпеку, доступність та гнучкість інфраструктури.

Windows Server є основою екосистеми Microsoft і продовжує використовуватися як головний елемент роботи підприємств.

Windows Server 2016 має засоби забезпечення безпеки, вбудовані в операційну систему. Нижче розглянуті найбільш значущі з них.

Стеження за діяльністю мережі:

Windows Server 2016 дає багато інструментальних засобів для стеження за мережевою діяльністю і використанням мережі. ОС дозволяє:

- проглянути сервер і побачити, які ресурси він використовує;

- побачити користувачів, підключених в даний час до сервера і побачити, які файли у них відкриті;

- перевірити дані в журналі безпеки;

- перевірити записи у журналі подій;

- вказати, про які помилки адміністратор має бути попереджений, якщо вони відбудуться.

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

Для всіх користувачів мережі підприємства передбачено своє ім'я і пароль.

Windows Server 2016 дозволяє визначити, що увійде до ревізії і буде записано в журнал подій безпеки всякий раз, коли виконуються певні дії або здійснюється доступ до файлів.

Елемент ревізії показує виконана дія, користувача, який виконав його, а також дату і час дії. Це дозволяє контролювати як успішні, так і невдалі спроби яких-небудь дій. Журнал подій безпеки для умов підприємства є обов'язковим, оскільки у разі спроби злому мережі можна буде відстежити джерело.

Насправді протоколювання здійснюється тільки у відношенні підозрілих користувачів і подій. Оскільки якщо фіксувати всі події, об'єм реєстраційної інформації, швидше за все, ростиме дуже швидко, а її ефективний аналіз стане неможливим. Стеження важливе насамперед як профілактичний засіб. Можна сподіватися, що багато хто утримається від порушень безпеки, знаючи, що їх дії фіксуються.

Права користувача:

Права користувача визначають дозволені типи дій для цього користувача. Дії, регульовані правами, включають вхід в систему на локальний комп'ютер, виключення, установку часу, копіювання і відновлення файлів сервера і виконання інших завдань.

У домені Windows Server 2016 права надаються і обмежуються на рівні домена; якщо група знаходиться безпосередньо в домені, учасники мають права у всіх первинних і резервних контроллерах домена.

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

Установка пароля і політика облікову сеансу:

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

Якщо користувачі примусово відключаються від серверів, коли час його сеансу закінчився, то вони отримують попередження якраз перед кінцем встановленого періоду сеансу. Якщо користувачі не відключаються від мережі, то сервер проведе відключення примусово. Проте відключення користувача від

робочої станції не відбудеться. Годинник сеансу на підприємстві не встановлений, оскільки співробітники можуть затриматися на роботі.

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

2.10 Матриця доступу

На підприємстві використовується такий варіант захисту інформації як опікунський захист даних. Опікун - це користувач, якому надані привілеї або права доступу до файлових інформаційних ресурсів, права доступу наведені в таблиці 2.4.

Кожен співробітник має один з восьми різновидів:

- R - дозвіл на відкриття файлів тільки для читання;
- W - дозвіл на відкриття файлів для запису;
- C - дозвіл на створення файлів на диску;
- D - дозвіл на видалення файлів;
- N - дозвіл на перейменування файлів;
- X - дозвіл на запуск програм.

Таблиця 2.4 - Матриця доступу

Суб'єкти доступу	Об'єкти доступу				
	Доступ до файлів в комп'ютерах ПК1-ПК10	Доступ до інформації сервера С1	Доступ до стандартних програм	Доступ до Internet	Доступ до електронної пошти
Директор	R,W,C,D,N	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D, N	R,W,C,D,N, X
Голова відділу технічного	R,W,C,D,N	R,W,C,N	R,W,C,D,N,X	R,W,C,D, N	R,W,C,D,N, X

забезпечення					
Системний адміністратор	R,W,C,D,N,X	R,W,C,N,X	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X
Спеціаліст з питань кібербезпеки	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X	R,W,C,D,N,X
Менеджери	R,W,C,D,N	R,W,N	R,W,C,D,N,X	R	R,W,C,N
Бухгалтери	R,W,C,D,N	R,W,N	R,W,C,D,N,X	R	R,W,C,N
Офіс менеджер	R,W,C,D,N	R,W,N	R,W,C,D,N,X	R	R,W,C,N

2.11 Вибір антивірусного захисту

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

При організації системи антивірусного захисту на підприємстві враховувалися наступні чинники риски:

1. Можливість створення нових вірусів з орієнтацією на протидію конкретним антивірусним пакетам і механізмам захисту, використання вразливостей системного і прикладного ПЗ приводять до того, що навіть тотальне застосування антивірусних засобів з актуальними антивірусними базами не дає гарантованого захисту від загрози вірусного зараження, оскільки можлива поява вірусу, процедури захисту від якого ще не додані в новітні антивірусні бази.

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

3. Установка оновлень без попереднього тестування створює ризики несумісності системного, прикладного і антивірусного ПЗ і може приводити до порушень в роботі. В той же час тестування приводить до додаткових затримок в установці оновлень і відповідно збільшує ризики вірусного зараження.

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

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

Некваліфіковані дії з віддзеркалення вірусної атаки можуть приводити до посилювання наслідків зараження, часткової або повної втрати критичної інформації, неповної ліквідації вірусного зараження або навіть розширення вогнища зараження.

У разі безпосередньої дії вірусу на систему, або при проведенні некваліфікованих лікувальних заходів може бути втрачена інформація або спотворено програмне забезпечення .

В умовах дії вказаних чинників тільки вживання крутих комплексних заходів безпеки по всіх можливих видах загроз дозволить контролювати постійно зростаючі ризики повної або часткової зупинки бізнес процесів в результаті вірусних заражень.

За результатами тестів, які приведені у таблиці 2.5 був обраний антивірусній пакет ESET Nod32, який заняв перше місце та відповідає технічним вимогам до захисту інформації від несанкціонованого доступу, сукупність яких визначається функціональним профілем захищеності (КА-2, ЦА-1, ЦО-1, ДС 1, ДЗ 1, ДВ 1, НР 2, НИ 2, НК 1, НО 1, НЦ-1, НТ-2) із рівнем гарантій Г 2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-9.

ESET Nod32 (далі Nod32). Цей пакет забезпечує централізований захист корпоративної мережі будь-якого масштабу. Сучасне рішення на базі технологій Nod32 для корпоративних мереж, є унікальний технічний комплекс з вбудованою системою централізованого управління антивірусним захистом в масштабі підприємства. Nod32 дозволяє адміністраторові, що працює як усередині мережі, так і на видаленому комп'ютері (через мережу Internet) здійснювати необхідні адміністративні завдання по управлінню антивірусним захистом організації.

Таблиця 2.5 - Порівняння антивірусних програм

Тест/Антивірус	ESET Nod32	Symantec Norton Anti-Virus	Avast Premium	McAfee VirusScan
Помилкові спрацьовування	58%	38%	56%	61%
Самозахисти антивірусів	100%	62%	87%	100%
Лікування активного зараження	85%	40%	63%	53%
Швидкодія	мінімальний вплив на швидкість операційної системи	найшвидші антивірусні сканери на вимогу	найшвидші антивіруси для роботи з офісними програмами	середня швидкість
Виявлення сучасних поліморфних вірусів	26 з 33 балів	14 з 33 балів	31 з 33 балів	21 з 33 балів
Виявлення антивірусів і антируткитов на виявлення і видалення сучасних руткитов	6.7 з 8 балів	5.5 з 8 балів	6.5 з 8 балів	5 з 8 балів

Основні можливості:

- проактивний захист і точне виявлення загроз. Антивірус NOD32 розроблений на основі технології ThreatSense®. Ядро програми забезпечує - проактивне виявлення всіх типів загроз і лікування заражених файлів (зокрема, в архівах) завдяки широкому застосуванню інтелектуальних технологій, поєднанню евристичних методів і традиційного сигнатурного детектування;

- Host Intrusion Prevention System (HIPS). Вдосконалена система захисту від спроб зовнішньої дії, здатних негативно вплинути на безпеку комп'ютера. Для моніторингу процесів, файлів і ключів реєстру HIPS використовується поєднання технологій поведінкового аналізу з можливостями мережевого фільтру, що дозволяє ефективно деактувати, блокувати і запобігати подібним спробам вторгнення;

- висока швидкість роботи. Робота антивіруса NOD32 не відбивається на продуктивності комп'ютера - сканування і процеси оновлення відбуваються практично непомітно для користувача, не навантажуючи систему;

- зручність. Антивірус NOD32 розроблений за принципом мінімальної навантаження на систему і займає не більше 44 Мб пам'яті;

- простота використання. Компактний і інтуїтивно зрозумілий призначений для користувача інтерфейс, мінімальні звернення до користувача при роботі роблять використання NOD32 простим і зручним;

- персональний файервол. Персональний файервол NOD32 забезпечує захист від зовнішніх вторгнень. Використання функції низькорівневого сканування трафіку, дозволяє файерволу відображати більшість атак, які могли б пройти непоміченими.

2.12 Удосконалення організаційних заходів щодо забезпечення інформаційної безпеки мережі

Для покращення захисту КМ ТОВ «ЯВІР ДНІПРО-1» потрібно виконати додаткові заходи:

1. Patch - патч

Найбільш прямим і найважливішим заходом є усунення лазівок в операційній системі регулярними оновленнями безпеки (патчами).

2. Сегментація мережі

Використання маршрутизаторів із вбудованими брандмауерами може обмежити вхідний трафік із надійних та ненадійних пристроїв. Крім того, це пропонує ізоляцію для захисту від горизонтального поширення шкідливого програмного забезпечення.

3. Захист операційної системи

Звичайне антивірусне програмне забезпечення працює в системі, що базується на підписах. Антивірусний механізм порівнює файли та активність із базою даних відомих підписів вірусів. У разі виявлення уражені файли видаляються або поміщуються на карантин. Ця модель має два слабкі місця: по-перше, кожна операційна система повинна часто оновлювати свою базу даних антивірусів, щоб виявляти нові віруси та хробаки та мати можливість забезпечити відповідний захист. По-друге, нові шкідливі програми та віруси, які використовують так звану вразливість нульового дня, не розпізнаються, оскільки в базі даних для них немає підпису. Отже, все більшого значення набувають альтернативні методи забезпечення цілісності для захисту промислових систем.

2.12.1 Обновлення ОС сервера

Для покращення захисту КМ потрібно слідкувати та проводити оновлення програмного забезпечення, в свою чергу це стосуються самого серверу С1.

Windows Server 2019 (WS 2019) заснована на Windows Server 2016 (WS 2016) та основні відмінності WS 2019 від WS 2016 - це оновлені інструменти та відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі «Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows Server 2019 Datacenter. Технічні вимоги», що визначаються функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1,

ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та має Експертний висновок №1090 дійсний з 20.02.2020:

1. У Windows Storage Space Direct (WSSD) були додані нові функції та інструменти:

- Тепер WSSD встановлюється тільки на обладнання, що входять до Hardware compatibility list;

- з'явилася технологія дедуплікації та стиснення для ReFS-томів;

- з'явилася офіційна підтримка persistent memory (storage-class memory (SCM));

- з'явився інструмент аналізу історії продуктивності Performance history;

- з'явилася можливість використання USB flash drive як свідка (witness);

- граничний обсяг сховища збільшено до 4 PB на кластер;

- з'явилася можливість ручного поділу slabs на певні сервери.

2. У Windows Server 2019 було оптимізовано систему управління контейнерами Linux, а також значно знижено обсяги образів контейнерів.

3. Агенти та компоненти системи Windows Defender ATP тепер встановлені.

Під час встановлення Storage Replica на Windows Server 2019 тепер не потрібно встановлювати Windows Data Center, а також у Storage Replica було додано підтримку Windows Admin Center і збільшено швидкість транзакційного лога.

Однак у WS 2019 є і абсолютно нові функції для Windows Server.

1. Storage Migration Service - це система міграції даних зі старих файлових серверів на віддалені та хмарні сховища. Тепер немає потреби використовувати такий інструмент, як robocopy та його аналоги. Storage Migration Service надає графічний засіб для інвентаризації даних на серверах Windows та Linux, а потім передає дані на нові сервери або віртуальні машини Azure.

За допомогою Storage Migration Service ви зможете з легкістю виконати такі дії:

- інвентаризація кількох серверів та їх даних;

- швидке перенесення файлів, загальних файлових ресурсів та конфігурацій безпеки з вихідних серверів;

- Управління однією або декількома процесами міграції з інтерфейсу користувача центру адміністрування Windows.

2. System Insights - це система прогнозної аналітики, яка базується на моделі машинного навчання. System Insights виконує локальний аналіз системних даних сервера, таких як лічильники продуктивності та події. System Insights надає прогнози як інтуїтивно зрозумілих графіків.

Завдяки System Insights можливо отримати детальний звіт про продуктивність сервера, скласти прогноз утилізації ресурсів, тим самим скоротити експлуатаційні витрати.

3. Удосконалена система безпеки. Нові можливості безпеки Windows Server 2019 поєднують у собі інші можливості безпеки ніж Windows Server 2016 в різних областях. Це забезпечує надійний захист від додаткових загроз. Розширений багаторівневий захист Windows Server 2019 надає комплексний захист, який в даний час необхідний серверам.

4. Сервер із захищеним ядром. Сертифіковане серверне обладнання із захищеним ядром від партнера оригінального виробника обладнання забезпечує додатковий захист від витончених атак. Це допомагає забезпечити підвищену надійність при роботі з критично важливими даними в деяких галузях, де важлива конфіденційність даних. Сервер із захищеним ядром використовує можливості обладнання, вбудованого програмного забезпечення та драйверів для увімкнення розширених функцій безпеки Windows Server. Багато з цих функцій доступні на комп'ютерах Windows із захищеним ядром, а також доступні при використанні серверного обладнання із захищеним ядром та Windows Server 2019.

5. Корінь довіри обладнання. Захищені мікросхеми криптопроцесорів довіреного платформного модуля 2.0 забезпечують безпечне апаратне сховище конфіденційних криптографічних ключів та даних, включаючи результати

вимірювання цілісності системи. Дозволяє переконатися, що сервер запущений з допустимим кодом і може бути довіреним під час подальшого виконання коду. Ця можливість називається коренем довіри обладнання та використовується такими функціями, як шифрування диска BitLocker.

6. Захист вбудованого ПЗ. Вбудоване ПЗ працює з високими привілеями і часто невидиме для традиційних антивірусних рішень, що призвело до збільшення кількості атак із відповідним напрямком. Серверні процесори із захищеним ядром підтримують можливості вимірювання та перевірки процесів завантаження за допомогою технології DRTM та ізоляції доступу драйверів до пам'яті за допомогою технології захисту DMA.

7. Безпечне завантаження UEFI - це стандарт безпеки, який захищає сервери від шкідливих програм rootkit. Безпечне завантаження гарантує, що сервер завантажує лише вбудоване програмне забезпечення та програмне забезпечення, довірене для виробника обладнання. При запуску сервера вбудоване програмне забезпечення перевіряє підпис кожного компонента завантаження, включаючи драйвери вбудованого програмного забезпечення та ОС. Якщо підписи дійсні, сервер завантажується, а вбудоване програмне забезпечення надає керування операційною системою.

8. Безпека на базі віртуалізації - VBS. Сервери із захищеним ядром підтримують технології захисту на основі віртуалізації та забезпечення цілісності коду на основі гіпервізора. Безпека на базі віртуалізації використовує функції апаратної віртуалізації для створення та ізоляції безпечної області пам'яті від звичайної операційної системи, захищаючи від цілого класу вразливостей, що використовуються в атаках майнінгу криптовалюти. VBS також дозволяє застосовувати Credential Guard, щоб облікові дані та секрети користувача зберігалися у віртуальному контейнері, до якого операційна система не може отримати доступ безпосередньо. HVCI використовує VBS для значного посилення дотримання політики цілісності коду, включаючи цілісність режиму ядра, яка перевіряє всі драйвери режиму ядра та двійкові файли у віртуалізованому середовищі перед запуском,

запобігаючи завантаженню непідписаних драйверів або системних файлів у системну пам'ять.

9. Захист даних ядра (KDP) забезпечує захист пам'яті ядра лише для читання з даними, де сторінки пам'яті захищені гіпервізором. KDP захищає ключові структури середовища виконання System Guard у Windows Defender від несанкціонованої зміни.

10. Безпечне підключення. Транспортування: протоколи HTTPS та TLS 1.3 за замовчуванням включені у Windows Server 2019.

Безпечні підключення є основою сучасних взаємозалежних систем. Transport Layer Security (TLS) 1.3 - це остання версія найпоширенішого протоколу безпеки в Інтернеті, що шифрує дані для забезпечення безпечного каналу зв'язку між двома кінцевими точками. Протоколи HTTPS і TLS 1.3 тепер увімкнені за промовчанням у Windows Server 2019. Вони захищають дані клієнтів, що підключаються до сервера. Це дозволяє відмовитися від застарілих алгоритмів шифрування та підвищити рівень безпеки порівняно з старішими версіями. Крім того, ці протоколи дають можливість шифрувати максимально можливу кількість підтверджень. Додаткові відомості про підтримувані версії TLS.

2.12.2 Оновлення апаратного забезпечення КМ

Міжмережевий екран або мережевий 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.

Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання - не пропускати (фільтрувати) пакети, не відповідні під критерії, визначені в конфігурації.

Деякі мережеві екрани також дозволяють здійснювати трансляцію адресів - динамічну заміну внутримережевих (сірих) адресів або портів на зовнішніх, використовуваних за межами локально обчислювальної мережі.

Це високотехнологічний маршрутизатор з підтримкою функції роутера Cisco RV325 (RV325-WB-K9-G5) дозволяє встановити велику кількість бездротових з'єднань у рамках роботи локальної мережі вашого бізнесу з високим рівнем відмовостійкості (рисунок 2.3), характеристики наведені в таблиці 2.6.

Ви зможете організувати більш інтелектуальну та інтегровану мережу з високою швидкістю, засновану на гнучких та адаптивних рішеннях згідно з останнім словом інтелектуальних технологій. Захист капіталовкладень, високий рівень продуктивності та вбудована система, що дозволяє знизити експлуатаційні витрати, та відмовитися від роутера та свіча старого покоління.

Рисунок 2.3 – Маршрутизатор Cisco RV325-WB-K9-G5

Таблиця 2.6 - Характеристики Cisco RV325-WB-K9-G5

Назва	Характеристики	
Cisco RV325-WB-K9-G5	Інтерфейси	24 x 10/100/1000 Мбіт/сек Gigabit Ethernet RJ-45 1 x 10/100/1000 Мбіт/сек Gigabit Ethernet RJ-45 інтернет (WAN) 1 x 10/100/1000 Мбіт/сек Gigabit Ethernet RJ-45 DMZ/інтернет (WAN)
	Швидкість LAN портів	1 Гбіт/с
	WAN-порт	Ethernet/USB
	Особливості	Підтримання VPN
	Підтримка протоколів	DHCP, IPsec, L2TP, NAT, PPPoE, PPTP

	Функції VPN	25 тунелів IPsec для під'єднання до філії 25 тунелів IPsec VPN через сторонні клієнти, такі як The GreenBow для під'єднання VPN віддаленого доступу 10 тунелів SSL VPN для віддаленого доступу до клієнта 10 тунелів PPTP для віддаленого доступу Стандарт шифрування даних (DES) Стандарт шифрування даних (3DES) Розширене шифрування (AES): AES-128, AES-192, AES-256 Аутентифікація: MD5/SHA1 IPsec NAT traversal: підтримується для тунелів клієнт-шлюз і шлюз-шлюз Розширення: виявлення (DPD), розділити DNS, резервування VPN, обмін ключами інтернету (IKE) із сертифікатом

Крім забезпечення високого рівня продуктивності провідних та безконтактних мереж, надає набір інтегрованих мережевих сервісів для максимально ефективної організації бізнес-процесів. Cisco RV325 ідеально підходить для створення та адміністрування засобів зв'язку на великих підприємствах або у великих офісах. Як додаткові сервіси цей пристрій пропонує запасний доступ до інтернету, а також можливість адміністрування з мобільних пристроїв. Ця лінійка маршрутизаторів забезпечує безпеку роботи мереж, захищає від можливого стороннього втручання та надає функції розмежування рівнів доступу до мереж. Всі бізнес-процеси будуть оптимізовані згідно з практичними завданнями завдяки сучасній модульній архітектурі приладу.

Лінійка пристроїв Cisco RV з потужних пристроїв безпеки містить функції брандмауеру, маршрутизатора та додатково VPN для критичних мереж. Ці високо рівневі функції «рівня 3» є життєво важливими для захисту промислової мережі від шкідливих атак або випадкових збоїв, а також для підключення до офісних або корпоративних мереж.

Функція моніторингу цілісності CIFS пропонує альтернативу звичайним антивірусним рішенням.

Моніторинг цілісності CIFS регулярно перевіряє системи, які працюють під керуванням Windows, визначаючи, чи не відбулися зміни певних даних,

наприклад файлів із розширенням .exe або .dll, порівняно з базовим станом. Якщо файли операційної системи Windows були змінені або видалені або файл доданий до відстежуваного каталогу, mGuard генерує сигнал тривоги у вигляді електронного листа, пастки SNMP або попередження. Тепер співробітники, що займаються розробкою, технічним обслуговуванням- або інформаційними технологіями, можуть вживати коригувальних заходів.

Для даної мережі і конфігурації сервера був вибраний апаратний міжмережевий екран Cisco RV325, який буде встановлений для захисту інформації, циркулюючої в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1», з боку Internet.

Cisco RV325 може забезпечити абсолютну безпеку внутрішньої мережі, повністю приховавши її від зовнішнього світу. На відміну від звичайних proxy-серверів, що виконують обробку кожного мережевого пакету окремо з істотним завантаженням центрального процесора, Cisco RV325 використовує спеціальну не UNIX-подібну операційну систему реального часу, забезпечуючи вищу продуктивність. Основою високої продуктивності міжмережевого екрану Cisco RV325 є схема захисту, що базується на застосуванні алгоритму адаптивної безпеки (adaptive security algorithm - ASA), який ефективно приховує адреси користувачів від порушників. Цей стійкий алгоритм забезпечує безпека на рівні з'єднання на основі контролю інформації про адреси відправника і одержувача, послідовність нумерації пакетів TCP, номери портів і додаткові прапори TCP.

Доступ через Cisco RV325 дозволений тільки в тому випадку, якщо з'єднання успішно пройшло ідентифікацію. Цей метод забезпечує прозорий доступ для внутрішніх користувачів і авторизованих зовнішніх користувачів, при цьому повністю захищаючи внутрішню мережу від несанкціонованого доступу. Завдяки застосуванню технології «крізного посередника» (Cut-Through Proxy) міжмережевий екран Cisco RV325 Firewall також забезпечує істотну перевагу в продуктивності в порівнянні з «екранами-посередниками» на базі ОС UNIX. Як і звичайні proxy-сервери, Cisco RV325 контролює встановлення з'єднання на рівні застосування. Після успішного проходження користувачем

авторизації доступу, відповідно до прийнятих правил безпеки, Cisco RV325 забезпечує контроль потоку даних між абонентами на рівні сесії. Така технологія дозволяє міжмережевому екрану працювати значно швидше, ніж звичайні proxy-екрани.

Міжмережевий екран Cisco RV325 підтримує більше 500000 одночасних з'єднань і, відповідно, забезпечує підтримку сотень і тисяч користувачів без зниження продуктивності.

Повністю завантажений RV Firewall може забезпечити пропускну спроможність 1,0 Гбіт/с, тобто істотно вище, ніж будь-який міжмережевий екран на базі ОС UNIX або ОС Microsoft Windows.

Міжмережевий екран RV забезпечує низьку вартість використання і супроводу. Користувачі, що не мають спеціальної підготовки, можуть швидко набудувати за допомогою простої графічної оболонки RV Device Manager (PDM), доступ до якої здійснюється за допомогою звичайного веббраузера. PDM - це застосування, що використовує http-сервер, вбудований в RV, і що підтримує основний набір команд, необхідний для початкового налаштування міжмережевого екрану. PDM дозволяє настроювати міжмережевий екран практично з будь-якого комп'ютера, для захисту пристрою від «злому під час конфігурації користувач може використовувати протокол SSL.

Міжмережевий екран Cisco RV325 також дозволяє уникнути проблеми браку адрес при розширенні і зміні IP-мереж, Технологія трансляції мережевих адрес Network Address Translation робить можливим використання в приватній мережі, як існуючих адрес, так і резервних адресних просторів.

Cisco RV325 також може бути настроєний для сумісного використання трансльованих і нетрансльованих адрес, дозволяючи використовувати як адресний простір приватної IP-сети, так і зареєстровані IP-адреса.

Основні можливості :

- система захисту від несанкціонованого доступу на рівні з'єднання забезпечує безпеку ресурсів внутрішньої мережі;

- технологія Cut Through Proxy дозволяє контролювати як вхідні, так і витікаючі з'єднання на базі таких протоколів безпеки, як Terminal Access Controller Access Control System (TACACS+ або Remote Access Dial-In User Service (RADIUS);

- до шести мережевих інтерфейсів для застосування розширених правил захисту. Графічний інтерфейс адміністратора Security Manager призначений для налаштування до 100 міжмережевих екранів RV Firewall з єдиної консолі;

- динамічна і статична трансляція адрес. Підтримка протоколу мережевого управління SNMP;

- облікова інформація з використанням ведення журналу системних подій (syslog);

- прозора підтримка всіх основних мережевих послуг, таких як World Wide Web (WWW), File Transfer Protocol (FTP), Telnet, Archie, Gopher.

- підтримка застосувань мультимедіа, включаючи Progressive Networks RealAudio & ReadVideo, Xing StreamWorks, White Pines CU-SeeMe, Vocal Tec Internet Phone, VDOnet VDOLive, Microsoft NetShow і VXtreme Web Theater.

- підтримка взаємодій Microsoft Networking сервер-клієнт, Oracle SQL Net-сервер-клієнт;

- безпечна вбудована операційна система реального часу;

- немає необхідності оновлення ПЗ на робочих станціях і маршрутизаторах;

- повний доступ до ресурсів мережі Інтернет для зареєстрованих користувачів внутрішньої мережі;

- сумісність з маршрутизаторами, що працюють під управлінням Cisco IOS™ ;

- підтримка відеоконференцій по протоколу H.323, включаючи Microsoft NetMeeting, Intel Internet Video Phone і White Pine Meeting Point;

- декілька можливих варіантів програмної і апаратної комплектації;

- засоби централізованого адміністрування;

- сповіщення про важливі події на пейджер або по електронній пошті.

- підтримка інтерфейсів Ethernet, Fast Ethernet, Token Ring і FDDI.

- підтримка віртуальних приватних мереж (Virtual Private Network) з використанням стандартної технології IPSec.

- висока продуктивність.

2.12.3 Система виявлення вторгнень

Підсистема моніторингу є базовим елементом багаторівневої системи захисту мережі і призначена для виявлення різних типів мережевих атак. Дана підсистема виявляє мережеві атаки за допомогою аналізу пакетів даних, що циркулюють в автоматизованій системі, а також подій, що відбуваються на серверах.

У якості можливих рішень даної підсистеми можуть виступати наступні:

- пакетний сніфер, встановлений на сервері;

- антивірусні засоби захисту, встановлено на серверах;

- система виявлення і запобігання атак, компоненти якої розподілено встановлені по мережі.

У таблиці 2.7 представлено аналіз кожного з типів виявлення мережевих атак.

Таблиця 2.7 - Порівняльній аналіз досліджених рішень, розглянутих з точки зору системи моніторингу мережевих атак

Критерій	Система моніторингу		
	Система виявлення і запобігання атак	Антивірусні засоби захисту	Пакетні сніфери
Можливість виявлення мережевих атак в автоматичному режимі	+	+	-
Можливість блокування виявлених мережевих атак	+	-	-
Наявність модульного принципу побудови	+	+	+
Наявність розподіленої архітектури	+	+	-
Додатковій захист	+	-	-
Легкість реалізації	-	-	+
Кількість переваг	5	3	2

За підсумками порівняльного аналізу даних рішень в якості підсистеми моніторингу пропонується впровадження системи виявлення і запобігання атак. Пропоноване рішення в якості підсистеми моніторингу дозволяє своєчасно виявляти та блокувати мережеві атаки. Такий підхід до побудови підсистеми моніторингу не надає ніякого впливу на пропускну здатність мережевого обладнання, тому що весь аналіз мережевого трафіку здійснюється на сервері, а також даний підхід не вимагає переналаштування існуючого мережевого обладнання.

Система виявлення вторгнень (СОВ) програмний або апаратний засіб, призначений для виявлення фактів неавторизованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Internet. Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем.

Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активності, яке може порушити безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки проти уразливих сервісів, атаки, направлені на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення комп'ютерних вірусові

Зазвичай архітектура СОВ включає:

- сенсорну підсистему, призначену для збору подій, пов'язаних з безпекою системи, що захищається;

- підсистему аналізу, призначену для виявлення атак і підозрілих дій на основі даних сенсорів;

- сховище, що забезпечує накопичення первинних подій і результатів аналізу;

- консоль управління, що дозволяє конфігурувати СОВ, спостерігати за станом системи, що захищається, і СОВ, переглядати виявлені підсистемою аналізу інциденти.

За результатами порівняльного аналізу систем виявлення і запобігання атак (таблиця 2.8) обрано RealSecure.

Система виявлення атак RealSecure розроблена американською компанією Internet Security Systems, Inc. і призначена для вирішення одного з важливих аспектів управління мережевою безпекою - виявлення атак. Система RealSecure - це інтелектуальний аналізатор пакетів з розширеною базою сигнатур атак, який дозволяє виявляти ворожу діяльність і розпізнавати атаки на корпоративній мережі. Система RealSecure побудована за технологією аналізу мережевих пакетів в реальному масштабі часу (real-time packet analysis) відноситься до систем виявлення атак, орієнтованих на захист цілого сегменту мережі (network-based).

Як тільки атака розпізнається відбувається сповіщення адміністратора через консоль управління або електронну пошту. Крім того, атака може бути зареєстрована в базі даних, а також всі операції при здійсненні атаки можуть бути записані для подальшого відтворення і аналізу. У разі здійснення атаки, яка може привести до виведення з ладу вузлів корпоративної мережі, можливе автоматичне завершення з'єднання з атакуючим вузлом або реконфігурація міжмережевих екранів і маршрутизаторів так, щоб надалі з'єднання з атакуючим вузлом були заборонені. Розподілена архітектура системи RealSecure дозволяє встановлювати компоненти системи так, щоб виявляти і запобігати атакам на мережу як зсередини, так і зовні.

Таблиця 2.8 - Таблиця порівнянь систем виявлення і запобігання атак

Критерій порівняння	OSSEC HIDS	IBM RealSecure	Snort
Метод виявлення	Сігнатурній	Сігнатурній, аналіз протоколів	Сігнатурній, аналіз протоколів
Наявність можливості віддаленого управління	+	+	-
Наявність розподіленої архітектури	+	+	-
Наявність механізмів відповідної реакції	-	+	+
Додатковій захист	SSL	SSL	SNMPv2

Система RealSecure використовує розподілену архітектуру і містить два основні компоненти RealSecure Detector і RealSecure Manager. Перший компонент відповідає за виявлення і реагування на атаки, і складається з двох модулів - мережевого і системного агентів. Мережевий агент встановлюється на критичний сегмент мережі і виявляє атаки шляхом «прослуховування» трафіку. Системний агент встановлюється на контрольований вузол і виявляє несанкціоновану діяльність, здійснювану на даному вузлі. Компонент RealSecure Manager відповідає за налаштування і збір інформації від RealSecure Detector. Управління компонентами системи RealSecure 6.5 можливо здійснювати як з централізованої консолі, так і за допомогою додаткового модуля, що підключається до системи мережевого управління HP OpenView (HP OpenView Plug-In Module).

Система RealSecure є одним з кращих рішень для захисту корпоративної мережі і наступних ключових можливостей:

- велике число розпізнаваних атак;
- завдання шаблонів фільтрації трафіку;
- централізоване управління модулями стеження;
- фільтрація і аналіз великого числа мережевих протоколів, в т.ч. TCP, UDP і ICMP;
- фільтрація мережевого трафіку по протоколу, портам і IP-адресам відправника і одержувача;
- різні варіанти реагування на атаки;
- аварійне завершення з'єднання з атакуючим вузлом;
- управління міжмережевими екранами і маршрутизаторами;
- завдання сценаріїв з обробки атак;
- генерація SNMP-послідовностей, що управляють, для управління системами HP OpenView(r), IBM NetView(r) і Tivoli TME10(r);
- запис атаки для подальшого відтворення і аналізу;
- підтримка мережевих інтерфейсів Ethernet, Fast Ethernet і Token Ring;
- відсутність вимоги використання спеціального апаратного забезпечення;

- робота з різними Cryptographic Service Provider;

- встановлення захищеного з'єднання між компонентами системами, а також іншими пристроями;

- наявність всеосяжної бази даних по всіх атаках, що виявляються;

- відсутність зниження продуктивності мережі;

- робота з одним модулем стеження з декількох консолей управління;

- різні формати звітів;

- простота використання і інтуїтивно зрозумілий графічний інтерфейс;

- невисокі системні вимоги до програмного і апаратного забезпечення.

Система RealSecure дозволяє виявляти велике число атак і інших контрольованих подій. Нижче описані основні типи контрольованих подій:

«Відмова в обслуговуванні». Будь-яка дія або послідовність дій, яка приводить будь-яку частину системи, що атакується, до виходу з ладу, при якому та перестає виконувати свої функції. Причиною може бути несанкціонований доступ, затримка в обслуговуванні і так далі Прикладом можуть служити атаки SYN Flood, Ping Flood, Windows Out-of-Band (WinNuke) і тому подібне

«Неавторизований доступ». Будь-яка дія або послідовність дій, яка приводить до спроби читання файлів або виконання команд в обхід встановленої політики безпеки. Також включає спроби зловмисника отримати привілеї, більші, ніж встановлені адміністратором системи. Прикладом можуть служити атаки FTP Root, E-mail WIZ і тому подібне

«Попередні дії перед атакою». Будь-яка дія або послідовність дій з отримання інформації З або Об мережі (наприклад, імена і паролі користувачів), використовувані надалі для здійснення неавторизованого доступу. Прикладом може служити сканування портів (Port scan), сканування за допомогою програми SATAN (SATAN scan) і тому подібне

«Підозріла активність». Мережевий трафік, що виходить за рамки визначення «стандартного» трафіку. Може указувати на підозрілі дії,

здійснювані в мережі. Прикладом можуть служити події Duplicate IP Address, IP Unknown Protocol і тому подібне

«Аналіз протоколу». Мережева активність, яка може бути використана для здійснення однієї з атак вищеназваних типів. Може указувати на підозрілі дії, здійснювані в мережі. Прикладом можуть служити події FTP User decode, Portmapper Proxy decode і тому подібне

Періодичне оновлення бази даних атак дозволяє підтримувати рівень захищеності Вашої корпоративної мережі на необхідному рівні.

Для точнішого настроювання системи RealSecure на роботу в мережевому оточенні, адміністратор безпеки може використовувати або один з восьми спочатку встановлюваних шаблонів, або створювати на їх основі свої власні шаблони, що зважають на специфіку Вашої корпоративної мережі. Всі знов створені шаблони можуть бути збережені для подальшого використання. Шаблони представлені нижчим.

«Максимум можливостей». Даний шаблон дозволяє використовувати абсолютно всі можливості модуля стеження системи RealSecure™, включаючи виявлення атак, аналіз протоколів, запис сесій і тому подібне

«Детектор атак». Даний шаблон дозволяє тільки виявляти атаки. Цей шаблон може бути використаний для виявлення і віддзеркалення атак на ресурси особливо критичних ділянок або вузлів мережі.

«Аналізатор протоколів». Даний шаблон є протилежним «детектору атак», тобто всі можливості по виявленню атак відключені і доступні тільки функції контролю мережевих протоколів. Вказаний шаблон може використовуватися адміністраторами для розуміння всіх процесів, що відбуваються в корпоративній мережі.

«Web-сторож». Даний шаблон дозволяє контролювати тільки HTTP-траффик мережі. Вказаний шаблон може використовуватися адміністраторами для визначення HTTP-траффика Вашої корпоративної мережі або для контролю цього трафіку в сегментах, в яких встановлені тільки вебсервера. При

використанні даного шаблону виявляються тільки атаки, засновані на використанні протоколу HTTP.

«Windows-сети». Даний шаблон дозволяє контролювати трафік, специфічний для Windows мереж. Вказаний шаблон можна використовувати, наприклад, в тих мережах, які побудовані на базі операційної системи Windows NT. При використанні даного шаблону виявляються тільки атаки, специфічні для мереж, побудованих на основі сімейства операційних систем Windows.

«Запис сесій». Даний шаблон дозволяє записувати сесії по протоколах Telnet, FTP, SMTP (електронна пошта) і NNTP (мережеві новини).

«Модуль стеження в DMZ». Даний шаблон орієнтований на функціонування модуля стеження в демілітаризованій зоні (DMZ).

«Модуль стеження до міжмережевого екрану». Даний шаблон орієнтований на функціонування модуля стеження за міжмережевим екраном.

Можливість установки модулів стеження на найбільш критичні ділянки Вашої мережі і можливість централізованого управління ними з єдиного робочого місця робить систему RealSecure незамінним помічником фахівців відділів технічного захисту інформації будь-якої організації. Також можливий доступ до одного модуля стеження одночасно з декількох консолей управління. Це дає можливість управляти модулем стеження декільком адміністраторам, що можливо знаходяться в різних підрозділах (наприклад, у відділі захисту інформації і управлінні автоматизації).

Система RealSecure має можливість за завданням різних варіантів реагування на виявлені атаки:

- запис факту атаки в реєстраційному журналі;
- повідомлення про атаку адміністратора через консоль управління;
- повідомлення про атаку адміністратора по електронній пошті;
- аварійне завершення з'єднання з атакуючим вузлом;
- запис атаки для подальшого відтворення і атаки;
- реконфігурація міжмережевих екранів або маршрутизаторів;
- посилка SNMP-послідовності, що управляють;

- завдання власних обробників атак.

Модуль стеження системи RealSecure™ може автоматично завершувати з'єднання з атакуючим вузлом. Дана можливість доступна тільки для з'єднань по протоколу TCP і полягає в посилці IP-пакета зі встановленим прапором RST. Вказаний вид реакції на атаки дозволяє запобігти багато загроз, здійснюваних багатьма типами атак.

Система RealSecure має можливість генерації послідовностей, що управляють, по протоколу SNMPv1 або передачу певних даних як можлива у відповідь дія на виявлену атаку або яку-небудь контрольовану системою несанкціоновану дію. Послана послідовність містить дані про час і тип виявленої атаки або несанкціонованої дії.

Дана можливість може використовуватися для додаткової обробки виявленої атаки засобами управління мережею типу HP OpenView, IBM NetView, Tivoli TME10 або будь-яких інших, що дозволяють обробляти вхідні послідовності, що управляють, по протоколу SNMP.

Запис атаки для подальшого аналізу. Дана можливість дозволяє проглядати заздалегідь записані дії, що виконуються зловмисником при атаці. Це дозволить не тільки зрозуміти і проаналізувати дії порушника, але і наочно продемонструвати керівництву організації потенційні загрози. Відтворення атаки для аналізу може бути здійснене як в реальному часі, так і з будь-якою заданою швидкістю. Для завдання специфічних реакцій на атаки, в системі RealSecure існує можливість визначення своїх власних обробників (наприклад, повідомлення адміністратора про атаку по пейджеру). Обробник атаки має бути будь-яким виконуваним файлом, який може запускатися з командного рядка.

Система RealSecure володіє дуже могутньою підсистемою генерації звітів, що дозволяє легко створювати різні форми звітів. Можливість деталізації даних полегшує читання підготовлених документів як керівниками організації, так і технічним фахівцями.

Створювані звіти можуть містити як докладну текстову інформацію про виявлені атаки, відсортовану по різних ознаках, так і графічну інформацію, що

дозволяє наочно продемонструвати рівень захищеності вузлів Вашої корпоративної мережі.

Вся інформація в створюваних звітах може бути відсортована по різних ознаках:

- по пріоритету (ступені риски) атаки;
- по IP-адресу відправника;
- по IP-адресу одержувача;
- по іменах контрольованих подій.

Вся інформація про виявлені атаки зберігається в базі даних. Це дозволяє ефективно організувати всю інформацію і забезпечити швидкий доступ до даних при створенні різних звітів. За допомогою підсистеми налаштування можливе підключення будь-якої бази даних, що має ODBC-драйвер. Ця можливість дозволить використовувати саме ту систему управління базами даних, яка застосовується у Вашій організації (наприклад, Microsoft SQL Server, Microsoft Access і тому подібне). Крім того, дана можливість дозволяє Вам використовувати всю інформацію про мережевий трафік у Ваших власних системах.

Крім того, система RealSecure додатково дозволяє:

- зберігати звіти на жорсткому диску;
- зберігати звіти в базі даних Lotus Notes;
- зберігати звіти в теці Microsoft Exchange;
- пересилати звіти за допомогою механізму Microsoft Mail (MAPI).

Інтуїтивно зрозумілий графічний інтерфейс і простота використання системи допоможе швидко і легко набудувати її з урахуванням вимог, що пред'являються у Вашій організації. Принципи функціонування системи не вимагають реконфігурації інших систем. Це вигідно відрізняє систему RealSecure™, наприклад, від міжмережевих екранів або засобів контролю «активного» коду (Java, ACTIVEX і тому подібне).

При використанні системи RealSecure зниження продуктивності мережі незначне (не більше 3-5%). Проблеми можуть виникнути при функціонуванні

модуля стеження на комп'ютері з мінімально необхідними системними вимогами і великій інтенсивності мережевого трафіку. В цьому випадку частина пакетів може бути пропущена без відповідної обробки.

2.12.4 Удосконалення резервування даних КМ

Ніхто не застрахований від того, що важливі дані можуть видалитися, пошкодитися і т.д. Звичайно, після того, як це вже сталося, махати руками пізно, необхідно заздалегідь захистити себе. Як це зробити? Все просто - використовувати резервне копіювання, його називають «бекап». Особливо це важливо тим, хто має свій сайт. У даній статті ми розглянемо, що означає резервне копіювання і навіщо воно потрібне.

Бекап, резервне копіювання являє собою процес створення копії важливих файлів на додатковому носії. Напевно кожен стикався з тим, що дані з комп'ютера можуть пошкодитися або зруйнуватися в принципі і якщо у вас немає копії, то відновити важливі документи неможливо. Отже, таке копіювання служить своєрідним рятівним колом, яке допоможе відновити потрібні дані. Крім того, бекап знадобитися і в разі, якщо основний пристрій недоступний. Наприклад ви здали свій комп'ютер в сервісний центр або втратили телефон. А якщо ми говоримо про сайт, то проблеми можуть виникнути з хостингом. Маючи резервну копію файлів можна видихнути, адже все найцінніше на місці.

Логічно, що скопійовані файли не потрібно зберігати на тому ж комп'ютері або ноутбуці. Важливо, щоб вони були на іншому додатковому пристрої.

Логічно, що таке копіювання не було б потрібно, якби файли не губилися і не пошкоджувалися. І тут потрібно розуміти, що впливає на втрату даних, які причини? Розглянемо найпоширеніші:

1. Проблеми з ПК. Наприклад поламався жорсткий диск. Він не попередить про те, що завтра він виходить з ладу. Не виключено, що диск

бракований. Флеш-пам'ять не надійний носій інформації. Запам'ятайте, що ненадійно довіряти важливі дані одному пристрою.

2. Різні програмні збої. Так як програми пишуть люди, а вони можуть помилятися, то не варто виключати і програмний збій. Він може вплинути на те, що ОС не завантажиться. А різного роду помилки легко стануть причиною пошкодження документів, інформації і ін.

3. Не варто виключати і той факт, що пристрій з інформацією можуть просто викрасти.

4. Програми-шкідники і віруси. Так як ми 99% свого часу проводимо в інтернеті, не варто забувати і про віруси. Файли можуть або видалити або зашифрувати. Говорячи про антивіруси, то вони не завжди можуть врятувати ситуацію.

5. Людський фактор. Так, як не дивно, але користувач може сам ненавмисно видалити свій документ, або забути куди поклав і як назвав.

Причини цілком логічні і кожен стикався хоча б раз з однією з ситуацій. Ті, хто встиг зробити резервне копіювання не особливо постраждали.

Існує кілька типів копіювання, розглянемо докладніше.

1. FTP-бекапи. Такий варіант копіювання передбачає під собою оренду певного обсягу дискового простору на FTP-сервері (сервер працює по протоколу передачі файлів). На такому носії простір розділено за допомогою різних облікових записів. Кожен користувач може завантажити на сервер необхідну кількість даних, але тільки за допомогою протоколу FTP. Зробити це можна вручну або використовуючи хостінгову панель.

2. CDP-бекапи. Дане скорочення з англійської перекладається як безперервний захист даних. Резервна копія створюється шляхом автоматичного збереження змінених даних. Тут схема полягає в наступному: встановлений CDP-агент розбиває жорсткий диск на блоки і передає дані по черзі на CDP-сервер (сховище резервних копій). Процес копії прискориться за рахунок того, що при наступних зверненнях будуть передаватися тільки ті блоки, в яких вже

відбулися зміни. Крім того, це дозволяє зменшити кількість використовуваного діалогового простору.

3. HDD-бекапи. Даний процес передбачає збереження копії даних на окремих жорстких дисках. Такий процес можна здійснювати або самостійно, або автоматизувати процес використовуючи спеціальне програмне забезпечення.

4. Хмарні бекапи. За назвою очевидно, що в такому варіанті файли зберігаються на хмарних сервісах, які представляють собою онлайн-сховище даних, об'єднаних в загальну мережу.

5. Снапшот (snapshot). Незважаючи на те, що снапшот є моментальний знімок файлів системи і не являє собою резервне копіювання в повному сенсі слова. Але при цьому всьому снапшот можна використовувати і в якості бекапа.

SnapShot являє собою знімок віртуальної машини в певний момент часу. На час зйомки робота комп'ютера зупиняється на секунду, після чого продовжує працювати в колишньому режимі. Здійснити цю процедуру можна або на сторінці з дисками, або на сторінці з віртуальними машинами. Перевага таких знімків в тому, що вони важать зовсім небагато і зберігаються вони на сторінці з дисками. Зроблені знімки між собою з'єднуються, утворюючи певний ланцюжок, видаляючи одне фото, «сусіди» об'єднуються. Можна робити близько 60 таких знімків, щоб нічого не упустити, але варто пам'ятати, що снапшот теж перевантажує ОЗУ.

Основний плюс використання саме такої системи в тому, що суть її роботи відрізняється від стандартного бекапа. Backup - тривалий процес архівування певної ділянки системи (або системи повністю). Він вимагає призупинення операцій над ділянкою файлів, які потрібно скопіювати. А ось якщо використовувати знімок файлів нічого зупиняти не потрібно.

Резервне копіювання важливе і не варто ігнорувати цей процес. Але важливо розуміти, що є певні файли, які необхідно дублювати в першу чергу.

- Фотографії та робочі документи;

- Різні замітки і контакти;

- Файли налаштувань необхідного ПЗ;

- Закладки браузера і інформація збережена з Мережі;

- Інші дані, які складно відновити. Не варто копіювати те, що можна легко знайти в Інтернеті (наприклад, музику, фільми і т.д.)

Якщо ми говоримо про ТОВ «ЯВІР ДНІПРО-1», то необхідно повністю копіювати всі його дані.

В ідеалі мати кілька копій, 3-4, при цьому вони повинні знаходитися на різних носіях (можна використовувати всі носії, які ми перерахували вище). Важливо запам'ятати золоте правило резервного копіювання: копії важливих даних необхідно зберігати в трьох різних місцях, на трьох різних носіях. Наприклад, одна копія на сервері в Інтернеті, друга на жорсткому диску, третя на флешці. Звичайно ви можете зберігати одну з копій в іншому місті, але це за бажанням. Але в будь-якому випадку пам'ятайте, що всі копії повинні перебувати окремо від вашого ПК.

Ми вже говорили про те, що зберігати бекап необхідно в надійному місці (але не поспішайте орендувати комірку у Швейцарському банку). Надійним місцем можна вважати зовнішній носій інформації.

Розглянемо кращі варіанти:

1. Зовнішній жорсткий диск. Надійне пристрій, але при цьому вимагає дбайливого догляду (він зовсім не любить падати зі столу).

2. DVD-диск. Такий носій не боїться падінь, але швидкість запису не найвища. А ось зручність запису залежить від якості самого диска.

3. Флешка, вона ж USB-накопичувач. Переваги: невеликий розмір, простота у використанні. Але не сильно надійні. Відразу відзначимо, що в ідеалі флешку використовувати як додатковий пристрій для резервного копіювання.

4. Хмара. Непоганий варіант, так як у користувача є можливість отримати дані з будь-якого пристрою, де є доступ в Інтернет.

Процес бекапа можна зробити вручну або використовувати спеціальну програму. До слова останній варіанти набагато спрощує копіювання. Але в будь-якому випадку, який би варіант ви не вибрали, будь-який з них зводиться до чотирьох простих дій:

- Підключити зовнішній накопичувач.
- Скопіювати необхідні дані.
- Обов'язково перевірити копію.
- Відключити накопичувач, через безпечний «вихід».

Щоб файли не займали багато місця, заархівуйте їх. Якщо ви вибираєте автоматичний варіант, то програма сама зробить це.

Очевидно, що копіювання файлів краще робити регулярно. Завдяки бекапу можна уникнути достатньої кількості проблем. Та й в принципі, будь-яка втрата важливого документа може призвести до складнощів.

Необхідно регулярно робити резервну копію важливих файлів і чим частіше ви будете робити бекап, тим менше роботи вам доведеться виконувати після відновлення.

Є кілька правил, або порад, які дозволять зробити процедуру бекапа правильною.

1. Робіть резервну копію регулярно. Очевидно, що чим частіше ви робите бекап, тим менше роботи доведеться виконувати після відновлення.

2. Має бути кілька копій на різних носіях. Крім того, один з варіантів повинен знаходиться в іншому будинку, квартирі, місті і.т.д. А взагалі, краще одну копію зберегти на жорсткому диску, а другу на хмарі. Так буде надійніше.

3. Після того як провели процедуру бекапа, відразу відключіть накопичувач від ПК, щоб уникнути впливу вірусів.

4. Краще робити резервну копію для всіх своїх пристроїв. Для ноутбуків, стаціонарних комп'ютерів, смартфонів і планшетів.

5. Кожен раз, перевіряти створені копії. Не виключена така ситуація: ви зробили бекап ПК, але не перевірили, що файли не читаються. Але проблема в тому, що про це ви дізнаєтеся лише при відновленні даних.

2.13 Висновки

В даному розділі був виконаний аналіз існуючої архітектури мережі ТОВ «ЯВІР ДНІПРО-1», проаналізовані інформаційні потоки мережі, а також існуюча система розмежування доступу. На основі проведеного аналізу були виявлені недоліки функціонування існуючої системи інформаційної безпеки мережі підприємства. Також були розглянуті та проаналізовані вимоги до системи інформаційної безпеки мережі і проведені дослідження можливих моделей моніторингу даних, циркулюючих у мережі. Після цього був здійснений порівняльний аналіз розглянутих моделей.

Базуючись на виконаних дослідженнях, були розроблені рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі підприємства, а також рекомендації та інструкції по безпосередній роботі з системою:

1. Обновити існуючу ОС сервера з платформи Windows Server 2016 на Windows Server 2019;

2. Придбати апаратний пристрій, міжмережевий екран Cisco RV325-WB-K9-G5 для заміні існуючого комутатора HP StorageWorks 8/8 SAN Switch AM867A та маршрутизатора Tp-link Ultra (KN-1810).

3. Придбання система виявлення атак RealSecure.

4. Запропоновані заходи покращення процесу копіювання та зберігання копій ІБ.

Цілі програми захисту інформації ТОВ «ЯВІР ДНІПРО-1» полягають в тому, щоб гарантувати цілісність, доступність і конфіденційність даних, які мають бути достатньо повними, точними, і своєчасними, щоб задовольняти виробничі потреби співробітників, не жертвуючи при цьому основними принципами, описаними в цій політиці. Визначаються наступні цілі:

- Гарантувати, що в середовищі ТОВ «ЯВІР ДНІПРО-1» забезпечується відповідна безпека, відповідна критичності інформації;

- Гарантувати, що безпека є рентабельною і заснована на співвідношенні вартості і ризики, або необхідно задовольняє відповідним керівним вимогам;

- Гарантувати індивідуальну підзвітність для даних, інформації, і інших комп'ютерних ресурсів, до яких здійснюється доступ;

- Гарантувати перевірку середовища копіювання інформації;

- Гарантувати, що службовці будуть забезпечені достатньо повним керівництвом по розподілу обов'язків щодо підтримки безпеки при роботі в автоматизованій інформаційній системі;

- Гарантувати, що для всіх критичних функцій компанії ТОВ «ЯВІР ДНІПРО-1» є відповідні плани забезпечення безперервної роботи, або плани відновлення при стихійних лихах.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка комплексної системи захисту інформації комп'ютерної мережі потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції - це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{mз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин} \qquad (3.1)$$

де $t_{mз}$ - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ - тривалість процесу аналізу ризиків;

$t_{вз}$ - тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ - тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ - тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=20годин, $t_в$=40 годин, $t_а$=20 годин, $t_{вз}$=15 годин, $t_{озб}$=8 годин, $t_{овр}$=6 годин, $t_д$=6 годин.

Отже: t = 20 + 40 + 20 + 15 + 8 + 6 + 6 = 115 годин

Розрахунок витрат на створення політики безпеки інформації.

Витрати на розробку політики безпеки інформації $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}, \quad грн. \tag{3.2}$$

$$З_{зп} = t * З_{іб} = 115 * 240 = 27600 \text{ грн.}$$

де t - загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ - средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, 240 грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t_д * С_{мч}, \quad грн. \tag{3.3}$$

де $t_д$ - трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ - вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,8 \cdot 6 \cdot 1,62 + \frac{6600 \cdot 0,4}{1920} + \frac{5150 \cdot 0,3}{1920} = 9,23 \text{ грн.}$$

Отже: $З_{мч}$= 115 * 9,23=1061,45 грн.

$$К_{рп} = З_{зп} + З_{мч} = 27600 + 1061,45 = 28661,45 \text{ грн.} \quad (3.4)$$

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі ТОВ «ЯВІР ДНІПРО-1», а також рекомендацій та інструкції по безпосередній роботі з системою планується використання антивірусу NOD32, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Серед апаратних засобів, які відповідно до розроблених рекомендації, необхідно придбати, належить міжмережевий екран Cisco RV325, який буде встановлений для захисту інформації, циркулюючої в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1», з боку Internet. Вартість міжмережевого екрану Cisco RV325 складає 18564 грн.

Також планується придбання система виявлення атак RealSecure, вартість якої складає 2100 грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \quad \text{грн.} \quad (3.5)$$

де $К_{пр}$ - вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ - вартість закупівлі ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ - вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, не потребуються, тому не враховується.

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки. Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто:

$$К_{н} = (18564 + 2100) * 0,2 = 4132,8 \text{ грн.}$$

$$К = 28661,45 + 18564 + 2100 + 4132,8 = 53458,25 \text{ грн.}$$

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.} \quad (3.6)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{єсв} + С_{ел} + С_{тос} + С_{ін}, \text{ грн.} \quad (3.7)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 5000 грн.).

Річні амортизаційні відрахування міжмережевого екрану Cisco RV325 вартістю 18564 грн із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$$С_а = 18564 / 2 = 15125 \text{ грн.}$$

Вартість подовження ліцензії антивірусу NOD32, який вже встановлений на 10 комп'ютерах підприємства, складає 1000 грн, $С_{ін}$=1000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.8)$$

В даному випадку в штаті ТОВ «ЯВІР ДНІПРО-1» вже є системний адміністратор, та спеціаліст с питання кібербезпеки ($С_з$ = 0 грн.).

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%.

$$С_{єсв} = 198000 * 0,22 = 43560 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.} \quad (3.9)$$

де Р - встановлена потужність апаратури інформаційної безпеки, (Р=1,4 кВт);

$F_р$ - річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ - тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,4 * 1920 * 1,68 = 4515,84 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% :

$$С_{тос} = К * 2\% = 53458,25 * 0,02 = 1069,17 \text{ грн.} \quad (3.10)$$

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 5000+15125+43560+4515,84+1069,17+1000 = 70270,01 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 70270,01 грн.

3.3 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.3.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ - час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ - заробітна плата обслуговуючого персоналу (системного адміністраторів), 12000 грн./міс.;

$З_с$ - заробітна плата сегмента корпоративної мережі (спеціаліста з питання кібербезпеки, 18000 грн./міс.;

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 10 осіб.;

О - обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 600 тис. грн. у рік;

$П_{зч}$ - вартість заміни встаткування або запасних частин, грн;

I - число атакованих сегментів корпоративної мережі, 1;

N - середнє число атак на рік, 40.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \qquad (3.11)$$

де $П_п$ - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_п = \frac{12000 \cdot 10}{176} \cdot 4 = 2727{,}27 \quad \text{грн.} \qquad (3.12)$$

де F - місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \qquad (3.13)$$

де $П_{ви}$ - витрати на повторне уведення інформації, грн.;

$П_{пв}$ - витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{12000 \cdot 10}{176} \cdot 6 = 4090{,}91 \text{ грн.} \qquad (3.14)$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{18000 \cdot 1}{176} \cdot 2 = 204{,}55 \text{ грн.} \qquad (3.15)$$

$$П_в = 4090{,}91 + 204{,}55 = 4295{,}46 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ}) \qquad (3.16)$$

$$V = \frac{600000}{2080} \cdot (4 + 2 + 6) = 3461{,}54 \text{ грн.}$$

де $F_г$ - річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 2727{,}27 + 4295{,}46 + 3461{,}54 = 10484{,}27 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \Sigma_i \Sigma_n U = \Sigma_1 \Sigma_{40} 10484{,}27 = 419370{,}8 \text{ грн.} \qquad (3.17)$$

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.} \qquad (3.18)$$

де B - загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R - вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

С - щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 419370,8 * 0,35 - 70270,01 = 76509,77 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці} \qquad (3.19)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К - капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{76509,77}{53458,25} = 1,43, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100) \qquad (3.20)$$

де $N_{деп}$ - річна депозитна ставка, (18 %);

$N_{інф}$ - річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,43 > (18 - 11)/100$$

$$1,43 > 0,07.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,43} = 0,7 \text{ років} \quad (3.21)$$

3.5 Висновок

Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «ЯВІР ДНІПРО-1» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 53458,25 грн., експлуатаційні 70270,01 грн. Величина річного економічного ефекту складає 76509,77 грн. Коефіцієнт повернення інвестицій ROSI складає 1,43 грн. Термін окупності капітальних інвестицій становить 7 місяців.

ВИСНОВКИ

У ході виконання роботи виконано аналіз існуючих мережевих систем моніторингу даних. Було проведено дослідження можливих варіантів використання засобів захисту інформації у комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1». На підставі проведеного дослідження визначені найбільш ефективні засобі захисту, механізм їх роботи та запропоновані заходи до покращення захисту КМ.

Практична цінність роботи полягає в підвищенні рівня інформаційної безпеки мережі ТОВ «ЯВІР ДНІПРО-1» шляхом впровадження засобів захисту інформації циркулюючої у мережі, а також удосконалення існуючої системи інформаційної безпеки мережі.

1. Обновити існуючу ОС сервера з платформи Windows Server 2016 на Windows Server 2019;

2. Придбати апаратний пристрій, міжмережевий екран Cisco RV325 для заміні існуючого комутатора HP StorageWorks 8/8 SAN Switch AM867A та маршрутизатора Tp-link Ultra (KN-1810).

3. Придбання система виявлення атак RealSecure.

4. Запропоновані заходи покращення процесу копіювання та зберігання копій ІБ.

У економічному розділі був здійснений розрахунок економічного ефекту від впровадження та налагодження розроблених засобів захисту інформації, які зменшать збитки від атак на мережу. На підставі отриманих результатів, коефіцієнта повернення інвестицій ROSI складає 1,43 грн./грн., і терміну окупності капітальних інвестицій до 7 місяців, було доведено, що впровадження в систему захисту пропонованої удосконалень в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1» є економічно ефективним рішенням.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994).

2 Закон України “Про захист персональних даних” (2010)

3 НД ТЗІ 1.1-004-99 „Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу”.

4 Домарьов В.В. Безпека інформаційних технологій. Методологія створення систем захисту. - К.: ТОВ ТІД ДС ISBN: 966-7992-02-0, 2001. -688 с.

5 ДСТУ 3396.1-96 Захист інформації. Технічний захист Інформації. Терміни та визначення.; Чинний від 01.01.98.

6 Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков - К.: Видавнича група BHV, 2009. - 608 с.

7 Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. - Запоріжжя: ГУ “ЗІДМУ”, 2003 - 250 с.

8 О. М. Черкун Сучасні технології комп’ютерної безпеки : колективна монографія. - Рівне : МЕГУ, 2012. - 90 с.

9 Одеський національний економічний університет. Інформатика та інформаційні технології : студентська наукова конференція, 20 квітня - 15 травня 2021 року 67с.

10 Безпека банківської діяльності : монографія / Н. Ф. Казакова, В. І. Панфілов, Л. М. Скачек, О. О. Скопа, В. О. Хорошко. - К.: ПВП «Задруга», 2013. - 282 с.

11 О. В. Орлик. Економічна безпека в умовах глобалізації світової економіки: Дніпропетровськ : «ФОП Дробязко С.І.», 2014. - Т. 2. - 268с.

12 О. В. Орлик. Modern problems of regional development: Collection of scientific articles. - 2014. - Vol. 2. - P. 190-194.

13 Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. - 2013. - № 15(204). - Ч. 1. - С. 59-62.

14 Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. - К.: Кондор, 2005. -382 с.

15 Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. 414 с.- К. : ДУІКТ, 2006. -закл.] / В.М. Богуш, А. М. Кудін.

16 Менаске Д. Продуктивність Web-служб. Аналіз, оцінка та планування / Менаске Д., 480 с. : ДіаСофтЮп", 2012. Віргіліо А. ; пров. з англ.

17 Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. - Х. : Вид. ХНЕУ, 2013. - 476 с.

18 Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. 2007. - 209 с. - К. : ПоліграфКонсалтинг. -Терейковський.

19 Щеглов А. Ю. Захист комп'ютерної інформації від несанкціонованого доступу/А. Ю. Щеглов. - К.: Наука та техніка, 2012. - 384 с.

20 Гундарь К. Ю. Защита информации в компьютерных системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевський. - К.: «Корнейчук», С. 200.- 152.

21 NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications//National Institute of Standards and Technology Special Publication 800-22rev1a, 2010, - 131 p.

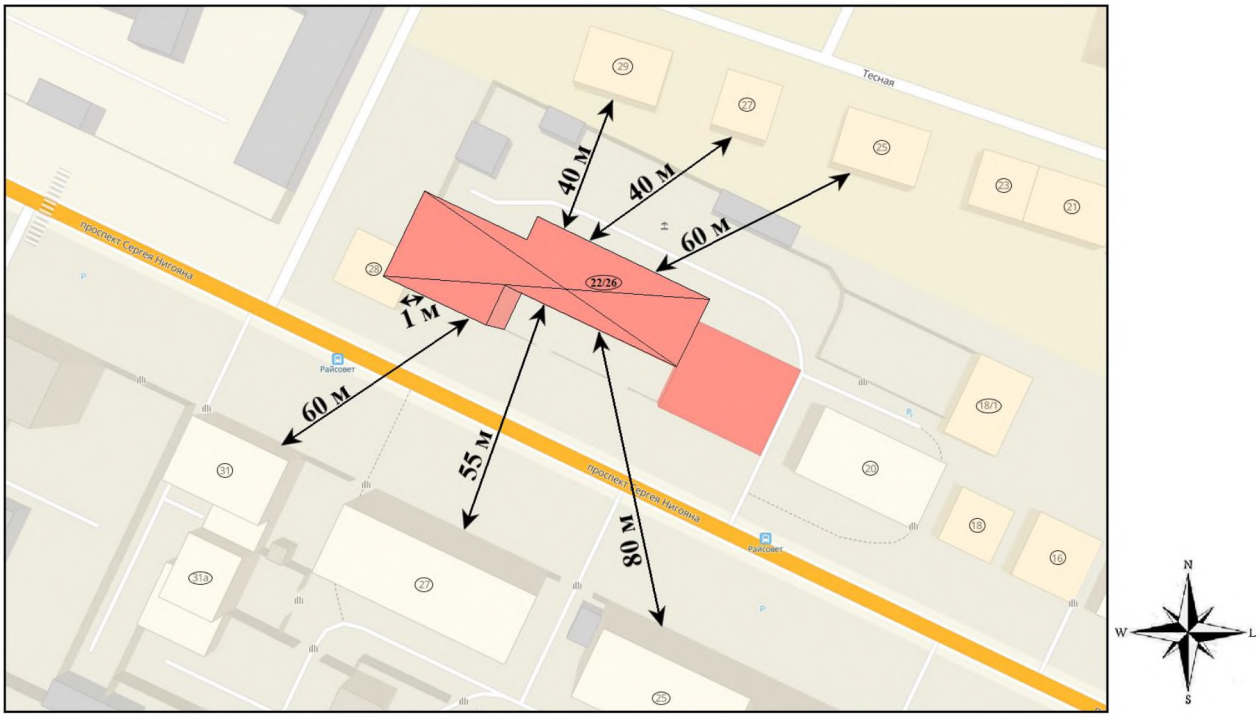
22 Internet для користувача : [навч. посіб.] / В. М. Антоненко, Б. Д. Пацай, Л. О. Терейковська, І. А. Терейковський ; Держ. податк. адмін. України, Нац. ун-т держ. податк. служби України. - Ірпінь : НУ ДПС України, 2010. - 244 с. : іл., табл. - Бібліогр.: с. 227. - Предм. покажч.: с. 242-244.

23 Комп'ютерне моделювання інформаційно-аналітичних систем / О. Г. Додонов, О. В. Коваль, Л. С. Глоба, Ю. Д. Бойко ; НАН України, Ін-т проблем реєстрації інформації. - Київ : ІПРІ НАН України, 2017. - 238 с. : іл. - Бібліогр.: с. 225-238.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	31	
6	А4	2 Розділ	45	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	
16	А4	Додаток Ж	1	

СИТУАЦІЙНИЙ ПЛАН
МАСШТАБ 1:500



ДОДАТОК Б

Умовні позначення ситуаційного плану:

Рисунок 1 – Розташування ТОВ «ЯВІР ДНІПРО-1»

ДОДАТОК В

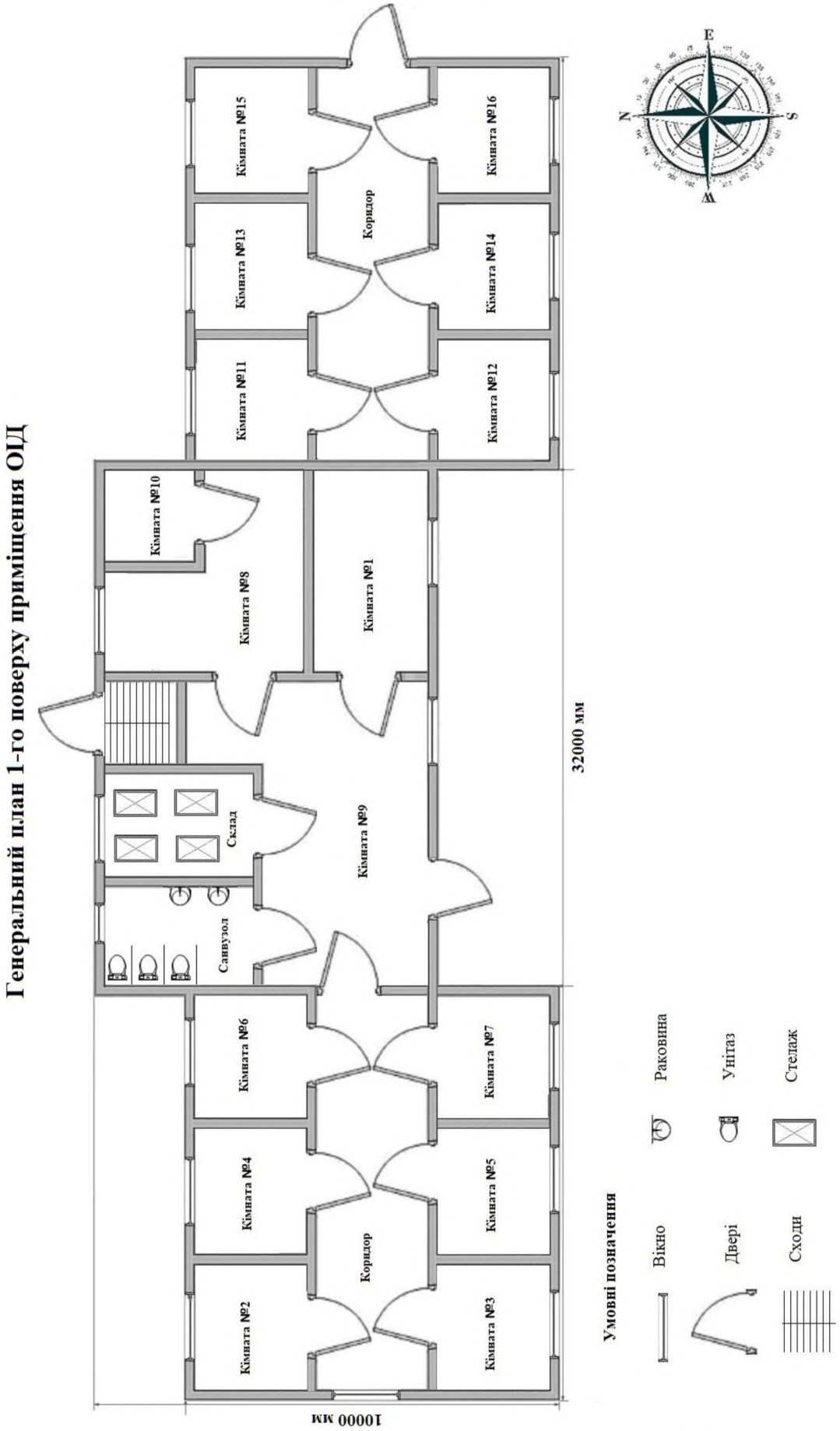


Рисунок 2 – Генеральний план 1-го поверху ОІД

ДОДАТОК Г

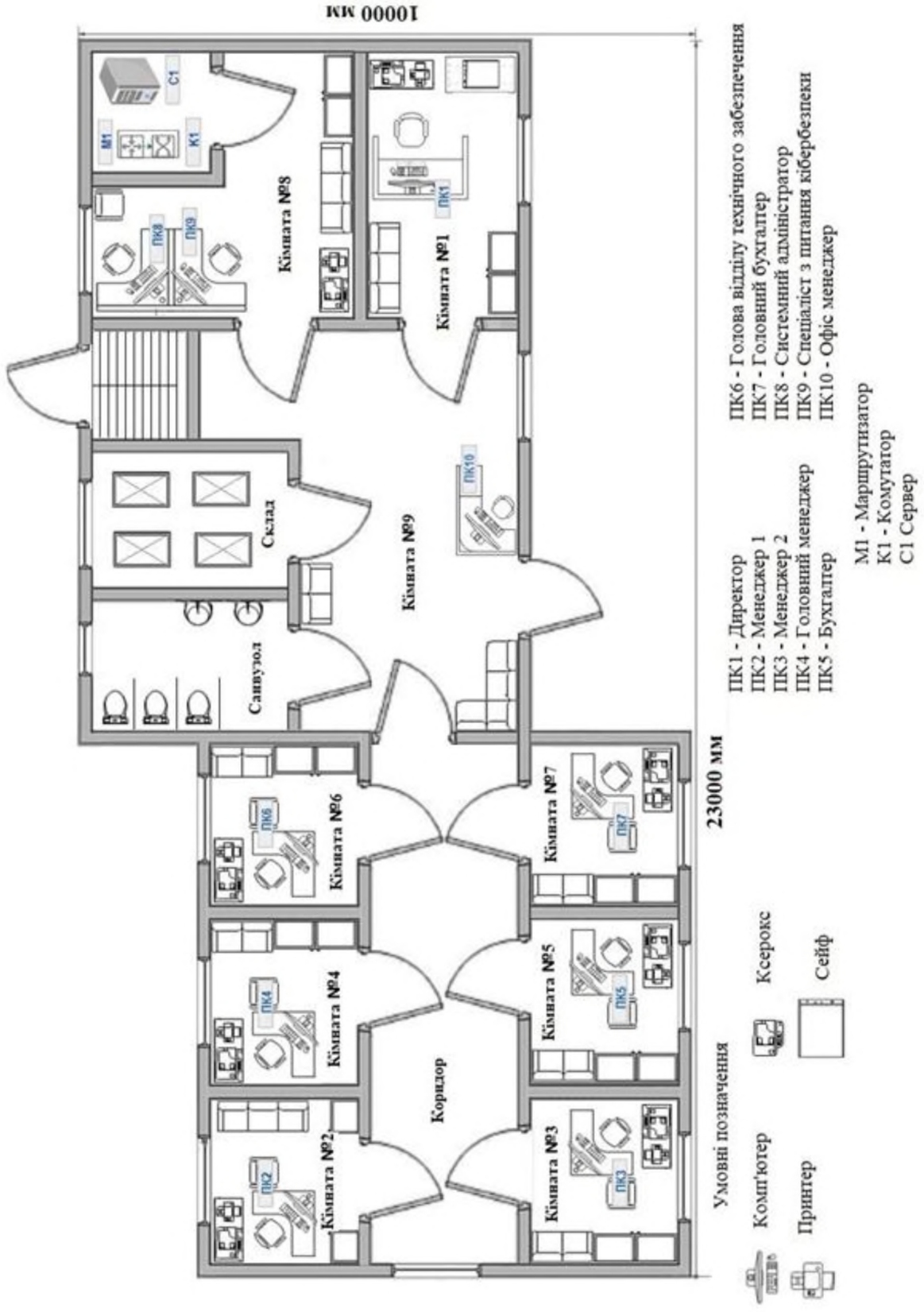


Рисунок 3 – Розміщення інформаційної системи ТОВ «ЯВІР ДНІПРО-1»

ДОДАТОК Д. Перелік документів на оптичному носії

1 Титульна сторінка.docx

2 Завдання.docx

3 Реферат.docx

4 Список умовних скорочень.docx

5 Зміст.docx

6 Вступ.docx

7 Розділ 1.docx

8 Розділ 2.docx

9 Розділ 3.docx

10 Висновки.docx

11 Перелік посилань.docx

12 Додаток А.docx

13 Додаток Б.docx

14 Додаток В.docx

15 Додаток Г.docx

16 Додаток Д.docx

17 Додаток Е.docx

18 Додаток Ж.docx

Презентація.pptx

ДОДАТОК Е. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Ж. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Обґрунтування засобів захисту інформації комп'ютерної мережі
товариства з обмеженою відповідальністю «ЯВІР ДНІПРО-1»

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 109 сторінках та містить 11 рисунків, 9 таблиць, 23 джерел та 7 додатка.

Об'єкт досліджень: інформаційна комп'ютерна мережа ТОВ «ЯВІР ДНІПРО-1» та шляхи її захисту.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1» від несанкціонованого доступу.

У розділі Стан питання. Постановка задачі описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У спеціальному розділі описана кратка характеристика об'єкту інформаційної діяльності ТОВ «ЯВІР ДНІПРО-1», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

В економічному розділі наведені розрахунки й обґрунтовані всі заходи щодо вдосконалення системи захисту інформації в комп'ютерній мережі ТОВ «ЯВІР ДНІПРО-1».

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію). Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник _____ _____

(підпис) (ініціали, прізвище)