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

Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Горянського Станіслава Владиславовича*

академічної групи *125-17-1*

спеціальності *6.170103 Управління інформаційною безпекою*

спеціалізації[1]

за освітньо-професійною програмою

на тему *Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Вектра»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер				

Дніпро
2021

ЗАТВЕРДЖЕНО:

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Горянському Станіславу Владиславовичу*** **академічної групи** ***125-17-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***6.170103 Управління інформаційною безпекою***
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Вектра»***

затверджену наказом ректора НТУ «Дніпровська політехніка» 317-с від 07.06.2021р

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи ТОВ «Вектра». Розробка моделі загроз.*	20.03.2021
Розділ 2	*Аналіз стану захищеності інформаційно-телекомунікаційної системи ТОВ «Вектра». Розробка політики безпеки інформації.*	30.05.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	15.06.2021

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 11.06.2021р.

Прийнято до виконання _____ Горянський С.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 85 с., 2 рис., 13 табл., 4 додатка, 15 джерел.

Об'єкт розробки: Розробка політики безпеки інформації інформаційно-комунікаційних системи концерну "Вектра"

Мета проекту: Розробка політики безпеки об'єкту інформаційної діяльності.

У загальній частині описаний об'єкт: рід діяльності, інформаційна система, інформаційні потоки, устаткування, програмне забезпечення. У технічному завданні виконаний, аналіз структури ІТС, аналіз загальної моделі погроз, визначений перелік порушників, інформаційних потоків і існуючих проблем у системі безпеки. Виконано вибір профілю захищеності підприємства.

У спеціальній частині були розроблені організаційні заходи, щодо забезпечення ОІД, була розроблена політика безпеки.

В економічній частині визначення витрат на провадження політики безпеки. Практичне значення проекту полягає в підвищенні інформаційної безпеки концерну "Вектра"

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, РИЗИКИ.

РЕФЕРАТ

Пояснительная записка: 85 с., 2 рис., 13 табл., 4 приложения, 15 источников.

Объект разработки: Разработка политики безопасности информации информационно-коммуникационных системы концерна "Вектра"

Цель проекта: Разработка политики безопасности объекта информационной деятельности.

В общей части описан объект: род деятельности, информационная система, информационные потоки, оборудование, программное обеспечение. В техническом задании выполнен, анализ структуры ИТС, анализ общей модели угроз, определен перечень нарушителей, информационных потоков и существующих проблем в системе безопасности. Выполнен выбор профиля защищенности предприятия.

В специальной части были разработаны организационные мероприятия по обеспечению ОИД, была разработана политика безопасности

В экономической части определения затрат на осуществление политики безопасности.

Практическое значение проекта состоит в повышении информационной безопасности информационно-коммуникационных системы концерна "Вектра"

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, РИСКИ

THE ABSTRACT

Explanatory note: 85 p., 2 fig., 13 table ., 4 applications. 15 of the sources.

Object of Development: Development of information security policy for information and communication systems of the concern "Vectra"

Project Objective: Develop a security policy object information activity.

A total of described object: type of activity, information systems, information flows, equipment, and software. The TOR is made, analysis of ITS analysis of the overall threat model defined list of offenders, information flows and existing problems in system security. Completed selection profile security company.

In the special part was developed organizational measures to ensure the OID was developed security policy

The economic definition of costs and expenses incurred Security Policy.

The practical significance of the project is to improve the information security of the concern "Vectra"

SECURITY POLICY, MODEL OF THREATS INFORMATION SECURITY, RISKS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ВАТ - відкрите акціонерне товариство;

ЕОТ - електронно-обчислювальна техніка;

ЗУ - закон України;

ІБ - інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД - несанкціонований доступ;

ОІД - об'єкт інформаційної діяльності;

ОС - операційна система;

ПБ - політика безпеки;

ПЕОМ - персональна електронно-обчислювальна машина;

ПЗ - програмне забезпечення;

ТЗІ - технічні засоби інформації;

ВСП - виробничо-структурний підрозділ

ЗМІСТ

ВСТУП

В наш час процес інформатизації набув глобального змісту. Інформатизація охоплює коло поточних і перспективних проблем – економічних, організаційних, соціальних, розвиток культури та освіти, діяльності всіх ланок соціального управління, кожної ланки господарювання.

Цей процес сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукоємних виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства. Тому питання державного регулювання сфери інформатизації стає усе більш актуальним та важливим для життя суспільства та держави.

В Україні процес інформатизації здійснюється згідно з Національною програмою інформатизації, яка визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення.

Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки (ІБ) на підприємствах, організаціях, в яких обробляється інформація з обмеженим доступом.

Одним з етапів побудови КСЗІ є розробка політики безпеки. Чим точніше буде створена політика безпеки, тим простіше буде адміністраторам безпеки розробити комплекс заходів для того, щоб запобігти успішним атакам. Важливу роль в розробці політики безпеки є визначення можливих загроз та порушень.

РОЗДІЛ 1.СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ТОВ "Вектра"

Об'єктом інформаційної діяльності (далі ОІД) є інформаційно-комунікаційних система концерну "Вектра"

Адреса: 14000, м. Дніпро , вул. Івана Акінфеєва 3.

Специфікація діяльності ОІД:

Відділи працюють за програмним забезпеченням інформаційно-комунікаційних системи концерну "Павлоград вугілля"

Щотижня передає аналітичні звіти про наземні і підземні роботи шахти до Павлоградського центрального офісу.

Час роботи понеділок-п'ятниця з 8:00-17:00, перерва 12:00 – 13:00, субота – неділя вихідні дні.

1.2 Обґрунтування необхідності створення КСЗІ

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

1.2.1 Категоріювання інформації

Згідно ЗУ «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. (пункт 1.4.1, таблиця 1.2)

1.2.2 Категоріювання ОІД

Згідно НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи-власника (розпорядника, користувача) об'єкта.

Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.

Категоріювання здійснюється за ознакою:

– ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД;

– об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися III категорія.

Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності.

Оскільки на ОІД обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія, (додаток А)

Простота і керованість інформаційної системи: принцип простоти і керованості інформаційної системи в цілому визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Забезпечення загальної підтримки мір безпеки: принцип загальної підтримки мір безпеки − носить нетехнічний характер. Рекомендується із

самого початку передбачити комплекс мір, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

1.2.3 Підстави для створення КСЗІ

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.

1.3 Обстеження ОІД

ОІД складається "Вектра" є 2 поверхова будівля.

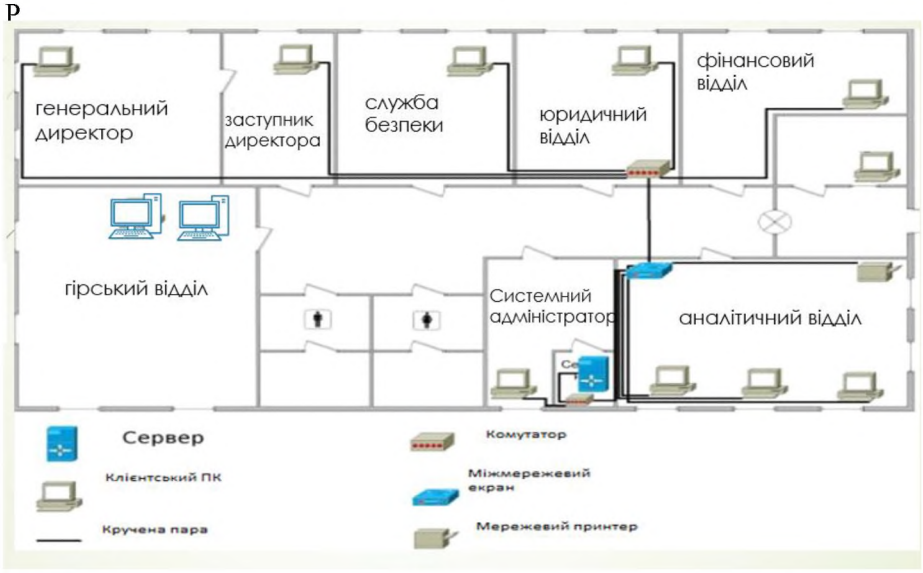
Централізовані системи опалення, водопостачання, водовідводу, вентиляції виходять за межі контрольованої зони. Вентиляція організована за допомогою вентиляційних труб.

Вікна: двостулковий метало-пластиковий склопакети у всіх приміщеннях розміром 1400х1320 мм. Віконні отвори обладнані регульованими пристроями типу: ролетні жалюзі.

Двері в приміщення металеві 2700х900. Дверні петлі захищені анти зрізами. Захисна металева внутрішня розсувна решітка на двері при вході до комп'ютерного центру.

Проведена телефонна лінія, яку надає ВАТ «ППТС». Комп'ютери кожного з відділів з'єднані в локальну мережу і мають вихід в Інтернет через безлімітне підключення від ВАТ «Київстар».

Р



исун ок 1.1 – «Век тра»

1.3.1 Анал із стру ктур и ІТС на ОІД

ІТС ОІД являє собою мережу типу «зірка», з виділеним сервером, побудовану з використанням одного комутатору. Структурна схема мережі представлена на рисунку 1.1.

ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має ADSL доступ до мережі Інтернет, який забезпечує ВАТ «Київстар». Відноситься до третього класу.

обчислювальна система у складі:

дев'ятнадцять ПЕОМ (Microsoft Windows 7 Максимальная з пакетом оновлення Service Pack 3– надалі Windows 7 SP3), об'єднаних між собою витою парою 5-ої категорії для внутрішньої прокладки ;

сервер управління доступом до мережі Інтернет з централізованим оновленням антивірусних баз і управлінням системними оновленнями;

активне мережеве обладнання (1 комутатор першого рівня на 24 портів);

програмні засоби активного мережевого обладнання, що реалізують спеціальні алгоритми управління мережею;

– прикладне ПЗ (Microsoft Office, Total Commander, WinRAR, Adobe Reader, Avast Endpoint Protection Suite Plus, Norton Personal Firewall 2004);

2) периферійні пристрої вводу\виводу даних Canon 1100;

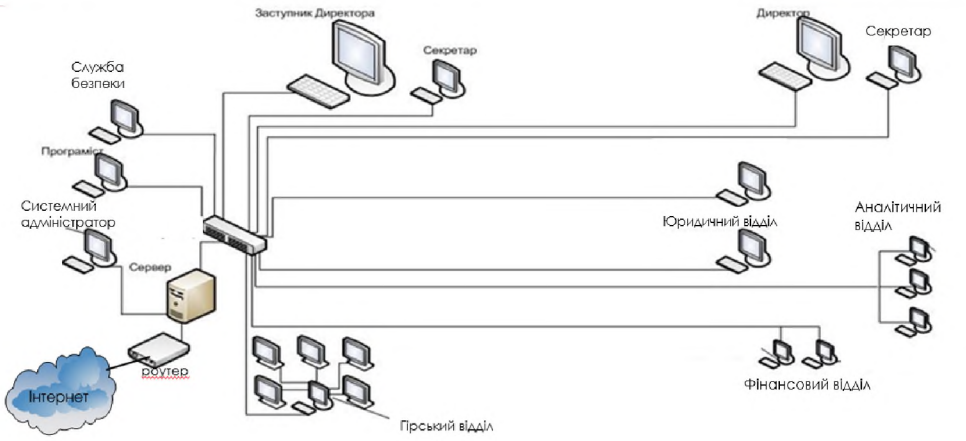
3) фізичне середовище − виділені приміщення підприємства, в яких розташована ІТС, що знаходяться у межах контрольованої зони;

4) користувачі ІТС:

– системний адміністратор мережі;

– користувачі з рівними повноваженнями;

5) в інформаційно-телекомунікаційній системі підприємства циркулює конфіденційна інформація, яка накопичується у базі даних та обробляється на робочих станція та зберігається на зовнішніх носіях, на які здійснюється архівування баз даних.



Рисунок

1.2 – ІТС «Вектра»

1.3.2 Загальна характеристика функціонування підприємства і мережі

ІТС ОІД являє собою мережу типу «зірка», з виділеним сервером, побудовану з використанням одного комутатору.

ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має ADSL доступ до мережі Інтернет, який забезпечує ВАТ «Київстар». Відноситься до третього класу.

1) обчислювальна система у складі:

– 19 ПЕОМ (Microsoft Windows 7 Максимальная з пакетом оновлення Service Pack 1– надалі Windows 7 SP1), об'єднаних між собою витою парою 5-ої категорії для внутрішньої прокладки;

–сервер управління доступом до мережі Інтернет з централізованим оновленням антивірусних баз і управлінням системними оновленнями;

–активне мережеве обладнання (1 комутатор на 24 порта);

–програмні засоби активного мережевого обладнання, що реалізують спеціальні алгоритми управління мережею;

–прикладне ПЗ (Microsoft Office, Total Commander, WinRAR, Adobe Reader, Avast Endpoint Protection Suite Plus, Norton Personal Firewall 2004);

– модем ZXV10H108L;

2) периферійні пристрої вводу\виводу даних Canon 1100;

3) фізичне середовище – виділені приміщення підприємства, в яких розташована ІТС, що знаходяться у межах контрольованої зони;

4) користувачі ІТС:

5) в інформаційно-телекомунікаційній системі підприємства циркулює конфіденційна інформація, яка накопичується у базі даних та обробляється на робочих станціях;

1.4 Аналіз загроз інформації, що циркулює на ОІД

1.4.1 Визначення інформаційних ресурсів, які потребують захисту

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді

Під інформацією Закон України «Про інформацію» [1] розуміє сукупність документованих або привселюдно оголошуваних відомостей про події або явища, що відбуваються у суспільстві, державі й навколишньому середовищі.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2] трактує інформацію як сукупність всіх даних і програм, використовуваних в автоматизованій системі, незалежно від способу їхнього подання.

Існує наступний поділ інформації з категорій важливості:

1) життєва важлива незамінна інформація, наявність якої необхідна для функціонування підприємства;

2) важлива інформація – інформація, що може бути замінена або відновлена, але процес відновлення дуже важкий і пов'язаний з більшими витратами;

3) корисна інформація – інформація, яку важко відновити, однак підприємство може ефективно функціонувати й без неї;

4) несуттєва інформація – інформація, що більше не потрібна підприємству.

На практиці віднесення інформації до однієї із цих категорій може являти собою дуже важке завдання, тому що та сама інформація може бути використана багатьма підрозділами підприємства кожне з яких може нести цю інформацію до різних категорій важливості. Категорія важливості, як і цінність інформації, звичайно змінюється згодом і залежить від ступеня відносини до неї різних груп споживачів і потенційних порушників.

Згідно закону України «Про інформацію» [1] за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.

Таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» захисту підлягає: відкрита інформація, яка є власністю держави і у визначенні Закону України «Про інформацію» належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (відкрита інформація). Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформаційний ресурс — сукупність документів у інформаційних системах.

Документом Закон України «Про інформацію» [1] передбачено матеріальну форму одержання, зберігання, поширення й використання інформації шляхом фіксації її на магнітній, кіно-, відео-, фотоплівці або на іншому носії. Поняття «документа» важливо, оскільки документи є частиною інформаційних ресурсів і мають юридичну значимість.

Інформація з обмеженим доступом (яка підлягає захисту) може оброблятися, передаватися та зберігатися за допомогою обчислювальних

ресурсів ІТС, а саме: серверів, робочих станцій, запам'ятовуючих пристроїв, периферійних пристроїв (принтерів, накопичувачів на змінних магнітних носіях інформації), мережевого обладнання, системного та функціонального ПЗ, засобів, що забезпечують взаємодію об'єктів ІТС.

Для ІТС концерну "Вектра" необхідний захист наступного інформаційного ресурсу:

1) файли, набори даних, які оброблюються, зберігаються і передаються в ІТС;

2) системне та функціональне ПЗ;

3) база даних з конфіденційними даними підприємства.

Інформаційні ресурси в ІТС циркулюють в обчислювальних засобах, а саме оперативно-запам'ятовуючий пристрій, дисковод, магнітні диски, дисплей, принтер (сканер), клавіатура, мережеве обладнання, які являються об'єктами захисту.

Таблиця 1.1 – Інформація що циркулює на ОІД

Інформація	Режим доступу	Правовий режим
1	2	3
Особові справи працівників	З обмеженим доступом	Конфіденційна
Внутрішні документи (накази, службові записки, інструкції)	З обмеженим доступом	Конфіденційна
Статутні документи	Відкрита	Відкрита
Відомості про фінанси, плани закупівель, перспективні плані підприємства	З обмеженим доступом	Конфіденційна

Зміст та характер договорів, контрактів, однією із сторін яких виступає підприємство	З обмеженим доступом	Конфіденційна
Аналітична інформація про видобуток корисних копалин	З обмеженим доступом	Конфіденційна
Аналіз активності обладнення.	З обмеженим доступом	Конфіденційна

Таблиця 1.2 – Визначення рівня конфіденційності, цілісності та доступності інформації

Інформація з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
	1	2	3
Особові справи працівників	К4	Ц3	Д0
Відомості про фінанси, перспективні плани підприємства	К1	Ц1	Д3
Договори , контракти, однією із сторін яких виступає підприємство	К1	Ц2	Д2
Плани закупівель	К2	Ц1	Д1
Стан роботи наземних і підземних машин, підйомника.	К2	Ц2	Д3

Конфіденційність:

– К0 - розголошення інформації призводить до краху роботи суб'єкта або дуже великих матеріальних втрат;

– К1-розголошення призводить до значних матеріальних втрат, якщо не буде вжито заходів;

–К2 - розголошення призведуть до деяких матеріальних втрат;

–К3 - Приносить матеріальний збиток в певних випадках;

–К4 - може принести малозначний збиток в рідкісних випадках;

Цілісність:

–Ц0 - призводить до неправильної роботи суб'єкта в цілому або значної його частини і наслідки зміни незворотні;

–Ц1 - несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки незворотні;

–Ц2 – несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки оборотні;

–Ц3 – несанкціоновані зміни не приведуть до збою в роботі суб'єкта, наслідки оборотні;

–Ц4 - несанкціоновані зміни не відражатимуться на роботі системи;

Доступність:

–Д0 - у разі порушення доступності інформації даного

типу підприємство не понесе матеріального збитку, робота підприємства не буде порушена, бажано впровадження, зміни в існуючих технологічних процесах;

–Д1 - у разі порушення доступності інформації даного типу підприємство понесе мінімальний збиток матеріального прибутку, робота підприємства не буде порушена, загальний дохід залишиться без зміни;

–Д2 - у разі порушення доступності інформації даного типу

підприємство понесе середній збиток матеріального прибутку за поточний квартал, робота підприємства не буде порушена, можливі відставання від конкурентних підприємств;

–Д3 - у разі порушення доступності інформації даного типу підприємство понесе збиток матеріального прибутку, робота підприємства буде ускладнена, загальний дохід може знизиться до половини існуючого;

–Д4 - у разі порушення доступності інформації даного типу підприємство понесе максимально велику шкоду матеріального прибутку протягом декількох кварталів, необхідно прийняття радикальних рішень стосовно доступності інформації на підприємстві;

1.4.2 Визначення переліку загроз

Загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС (НД ТЗІ1.1-003-99 [3]).

Загрози в залежності від виду впливів на інформацію й НСД до неї можна розділити на випадкові й навмисні.

До випадкових загроз варто віднести:

–відмови й збоїв апаратури;

–перешкоди на лінії зв'язку від впливів зовнішнього середовища;

–помилки людини як ланки системи;

–системні й системотехнічні помилки розробників;

–структурні, алгоритмічні й програмні помилки;

–аварійні ситуації й інші впливи.

–відмова від функціонування ІТС в цілому, наприклад вихід з ладу електроживлення;

–стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки

й т.д.

Навмисні загрози пов'язані з діями людини, причинами яких можуть бути певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес або проста розвага із самоствердженням своїх здатностей, як у хакерів, й т.д.

Таблиця 1.3 – Перелік загроз та визначення можливих порушень властивостей інформації

Загроза	Які властивості інформації порушуються		
	К	Ц	Д
	1	2	3
Загрози антропогенного характеру			
Крадіжка: 1) технічних засобів; 2) носіїв інформації; 3) інформації; 4) засобів доступу (ключі, паролі).	+	+	+
Підміна (модифікація): 1) операційних систем; 2) систем управління базами даних; 3) прикладних програм; 4) інформації (даних), заперечення факту відправки повідомлень; 5) паролів і правил доступу.	+	+	+

Знищення (руйнування): 1) технічних засобів (вінчестерів, системних блоків); 2) носіїв інформації (паперових, магнітних, оптичних); 3) програмного забезпечення (ОС,СУБД, прикладного ПЗ); 4) інформації (файлів, даних); паролів і інформації.	-	+	+
Знищення (руйнування): 1) технічних засобів (вінчестерів, системних блоків); 2) носіїв інформації (паперових, магнітних, оптичних); 3) програмного забезпечення (ОС,СУБД, прикладного ПЗ); 4) інформації (файлів, даних); паролів і інформації.	-	+	+
Техногенні загрози			
Порушення нормальної роботи (переривання): 1) швидкості обробки інформації; 2) пропускної здатності каналів зв'язку; 3) обсягів вільної оперативної пам'яті; 4) обсягів вільного дискового простору; 5) електроживлення технічних засобів; 6) хакерські атаки через глобальну мережу Інтернет.	-	-	+

Перехоплення інформації (несанкціоноване): 1) за рахунок ПЕМВ від технічних засобів; 2) при підключенні до каналів передачі інформації; 3) за рахунок порушення встановлених правил доступу; 4) занесення вірусу в робочі станції; 5) хакерські атаки.	+	+	-
Помилки: 1) при інсталяції ПЗ, ОС, СУБД; 2) при експлуатації ПЗ; 3) при експлуатації технічних засобів; 4) недбале ставлення співробітників до документації; 5) помилки при введенні даних.	-	+	+
Порушення нормальної роботи: 1) порушення працездатності системи обробки інформації; 2) порушення працездатності зв'язку; 3) старіння носіїв інформації і засобів її обробки; 4) порушення встановлених правил доступу; 5) електромагнітний вплив на технічні засоби.	-	+	+
Знищення (руйнування): 1) програмного забезпечення, ОС, СУБД; 2) засобів обробки інформації.	-	+	+

Модифікація (зміна): 1) програмного забезпечення, ОС, СУБД; 2) інформації при передачі по каналах зв'язку і телекомунікацій.	+	+	+
Стихійні загрози			
1) Аварії, пожежі, урагани; 2) Непередбачувані ситуації, нез'ясовні явища, інші форс-мажорні обставини.	-	+	+

1.4.3 Визначення переліку порушників

Порушник - це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Відносно ІТС порушники можуть бути: внутрішніми (з числа персоналу або користувачів системи), або зовнішніми (сторонніми особами).

Користувач інформації в системі - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі ІТС, особи, що мають доступ до неї, поділяються на наступні категорії:

− користувачі, яким надано повноваження розробляти й супроводжувати систему захисту інформації, а також повноваження забезпечувати управління ІТС - адміністратор мережі;

− користувачі, яким надано право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів – директор, начальник відділу кадрів, працівники відділу кадрів, головний економіст, економісти, секретар;

– розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

– постачальники обладнання і технічних засобів ІТС та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;

– технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища ІТС - інженер, електрики, технічний персонал з обслуговування будівель, ліній зв'язку.

Модель порушника – абстрактний формалізований або неформалізований опис порушника. Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

Таблиця 1.4 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника
К0	Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування

К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем.
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки.
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

Таблиця 1.5 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника
Ч1	До впровадження АС або її окремих компонентів.
Ч2	Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
Ч3	Під час функціонування АС (або компонентів системи).
Ч4	Як у процесі функціонування АС, так і під час зупинки компонентів системи.

Таблиця 1.6- Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника
Д1	Без доступу на контрольовану територію організації.
Д2	З контрольованої території без доступу у будинки та споруди.
Д3	Усередині приміщень, але без доступу до технічних засобів АС.
Д4	З робочих місць користувачів АС.
Д5	З доступом у зони даних (баз даних, архівів й т.ін.).
Д6	З доступом у зону керування засобами забезпечення безпеки АС.

Таблиця 1.7 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення
М1	Безвідповідальність
М2	Самозатвердження
М3	Корисливий інтерес

Таблиця 1.8 – Визначення переліку порушників за можливими мотивами, місцем, часом дії та категорією обізнаності

Посада	Можливий мотив	Категорія обізнаності порушника	Можливе місце дії	Можливий час дії

	1	3	3	4
Внутрішні				
Директор	М2,М3	К1	Д6	Ч4
Зас. директора	М2, М3	К2	Д5	Ч4
Працівники відділу кадрів	М1,М2, М3	К1	Д4	Ч3
Головний механік Головний інженер Гірничий відділ	М2,М3	К2	Д5	Ч4
Відділ Аналітики	М2,М3	К2	Д4	Ч3
Бухгалтери Відділ ВТБ	М1,М2, М3	К1	Д4	Ч3
Секретар	М1,М2, М3	К1	Д4	Ч3
Програміст	М1,М2, М3,	К4	Д6	Ч4
Системний адміністратор	М2, М3	К5	Д6	Ч4
Прибиральниця	М2, М3	К0	Д3	Ч2

Продовження таблиці 1.8

Зовнішні				
Представники організацій, що взаємодіють з питань технічного забезпечення	М3	К5	Д2	Ч1
Представники організацій, що взаємодіють з питань ПЗ	М3	К4	Д3	Ч1
Хакери	М2, М3	К3	Д1	Ч3

1.4.4 Визначення каналів несанкціонованого доступу до ІТС

Несанкціонований доступ до інформації - доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

Доступ порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Витік інформації - неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання (ДСТУ 3396.2-97 [4]).

Основними каналами витоку інформації в ІТС на ОІД є :

1) змінні носії, та носії на які здійснюється архівування;
2) робочі станції працівників відділів;
3) робоча станція адміністратора системи;
4) засоби вводу\виводу інформації;
5) канали передачі інформації в ІТС;
6) комутатор.
7)

1.4.5 Вибір заходів захисту інформації в ІТС підприємства

Забезпечення безпеки інформації в ІТС досягається шляхом застосування комплексу заходів щодо захисту інформації: організаційних, організаційно-технічних, застосування програмних, апаратних та програмно-апаратних засобів захисту, застосування технічних засобів захисту.

Згідно НД ТЗІ 1.1-003-99 [3] матриця доступу — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС одного типу (об’єктів-користувачів, об’єктів-процесів чи пасивних об’єктів), і містить визначені права доступу суб’єктів до кожного із типів об’єктів.

Згідно з Законом України „Про захист інформації в інформаційно-телекомунікаційних системах”[2].

Доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Таблиця 1.9 – Матриця керування доступом

1	2	3	4	5	6	7	8
С1	Ч,К,З, М,Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д, Зн
С2	Ч,К,З, М,Д, Зн	Ч,К,З,М, Д, Зн	Ч,К,З,М, Д,	Ч, З	Ч	-	Ч,К,З,Д
С3	Ч,К,З, М,Д	Ч,З,Д	Ч,З	Ч,З	Ч	-	Ч,К,З,Д
С4	-	-	-	Ч,З	Ч,З,Д	Ч,К,З,М, Д, Зн	Ч,К,З,Д
С5	-	-	-	Ч,З	Ч,З	Ч,К,З,М, Д, Зн	Ч,К,З,Д
С6	-	-		Ч,З	Ч,З	Ч,К,З,М, Д, Зн	Ч,К,З,Д
С7	-	-	Ч,З	Ч,З	Ч,К,З,Д	Ч,З	Ч,К,З,Д
С8	Ч,К,З, Д	Ч,З,Д	Ч,З,Д	Ч,З	Ч,З	-	Ч,К,З,Д
С9	-	-	-	Ч,З	Ч,З	-	Ч,К,З,Д
С10	Ч,К,З, Д	Ч,К,З,Д	Ч,К,З,Д	Ч,З,Д	Ч,З,Д	Ч,З,Д	Ч,К,З,Д

С11	-	-	-	Ч,К,З,Д	-	-	Ч,К,З,Д
С12	-	-	-	Ч,К,З,Д	-	-	Ч,К,З,Д

Позначення:

1) Суб'єкти доступу

–С1 - Директор

–С2 - Заступник директора

–С3 - Працівники відділу кадрів

–С4 – Аналітичний відділ

–С5 - Головний інженер

–С6 - Гірничий відділ

–С7 - Відділ контролю добичі

–С8 - Бухгалтер

–С9 - Відділ ВТБ

–С10 - Секретар

–С11 - Програміст

–С12 - Системний адміністратор

2) Об'єкти доступу:

–О1 - Особові справи працівників

–О2 - Трудові договори

–О3 - Відомості про інформацію

–О4 - Плани підприємства (плани закупівель, продажу, поточні і перспективні плани підприємства)

–О5 - Плани про видобуток вугілля

–О6 - Стан роботи наземних і підземних машин

–О7 - Статутні документи

3) Операції з файлами

–Ч - читання

–К - копіювання

–З - зберігання

– М - модифікація

– Д - друкування

– Зн - знищення

1.4.6 Критерії впровадження системи

Обраний профіль захищеності (опис послуг безпеки приведений у таблиці 1.10, критерії захищеності в таблиці 1.11):

3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 1.10 - Профіль захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-1(мінімальна конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність

		при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	7	

Продовження таблиці 1.10

1	2	3
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1(автентифікація вузла)

Таблиця 1.11 Критерії захищеності

Критерії захищеності	Чим реалізуються до впровадження політики безпеки	Чим реалізуються після впровадження політики безпеки
1	**2**	**3**
КД-2	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory

КО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
КВ-1	Використання протоколу SSL	Використання протоколу SSL
ЦД-1	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory
ЦО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
ЦВ-1	-	Використання засобів криптозахисту
ДР-1	Вбудовані засоби Windows	Вбудовані засоби Windows

Продовження Таблиці 1.11

1	2	3
НР-2	Вбудований журнал реєстрації Windows	Вбудований журнал реєстрації Windows
НИ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НК-1	-	Мережевий протокол автентифікації
НО-2	-	Призначення адміністратора безпеки
НЦ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НТ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НВ-1	-	Мережевий протокол автентифікації

Базова довірча конфіденційність (КД-2)

Послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів.

Політика довірчої конфіденційності поширюється наоб'єкти і забезпечує взаємодію зазначених об'єктів:

–користувачів усіх категорій;

–об'єкти, які містять конфіденційну інформацію, за умови визначення в АС груп користувачів з однаковими повноваженнями стосовно такої інформації і тільки в межах цих груп;

–всі інші об'єкти, які підлягають захисту, але не належать до зазначених вище видів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується об'єктів, які створюються користувачем у процесі виконання ним функціональних обов'язків.

КЗЗ повинен реалізувати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу, як власнику процесу, можливість визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

Повторне використання об'єктів (КО-1)

Послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від використання його попереднім користувачем або процесом.

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів ЛОМ, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами ЛОМ та прикладними процесами, що виконуються в ЛОМ.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках (ЖМД), якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту (імпорту) конфіденційної інформації з (в) ЛОМ та створенні «твердих» копій тощо.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Вимога цієї послуги в повному обсязі поширюється і на розділювані одночасно декількома користувачами процеси.

Мінімальна конфіденційність при обміні (КВ-1):

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Мінімальна довірча цілісність (ЦД-1)

Послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь-якої категорії

керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильнозв'язані об'єкти, які створюються користувачем у процесі виконання ним функціональних обов'язків. Користувач, який створив об'єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Обмежений відкат (ЦО-1)

Послуга забезпечує можливість відмінити окрему операцію або послідовність операцій й повернути захищений об'єкт, з яким маніпулював користувач, до попереднього наперед визначеного стану.

Політика обмеженого відкату забезпечує взаємодію нижчезазначених об'єктів і поширюється на:

–користувачів усіх категорій;

–сильно та слабозв'язані об'єкти, які містять конфіденційну інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

Факт використання користувачем послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з

журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки .

Мінімальна цілісність при обміні (ЦВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти крипостійкість використовуваних алгоритмів шифрування.

Використання ресурсів (ДР-1)

Послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти і забезпечує взаємодію цих об’єктів, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об’єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

Ручне відновлення після збоїв (ДВ-1)

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти та забезпечує їх взаємодію:

–системне та функціональне ПЗ;

–засоби захисту інформації та засоби управління КСЗІ;

–засоби адміністрування та управління обчислювальною системою;

–окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації.

Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування ЛОМ або окремих її компонентів, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна

Повторна інсталяція автоматизованої системи.

Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

Захищений журнал -(НР-2)

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів.

Політика реєстрації поширюється та забезпечує взаємодію користувачів усіх категорій.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

– вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;

– реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії із системи;

– зміна паролю користувачем будь-якої категорії;

– отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні конфіденційної інформації;

– виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку;

– копіювання наборів даних із інформацією конфіденційного характеру на запам'ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання інформації конфіденційного характеру на запам'ятовуючих пристроях, які згідно з політикою безпеки для цього не призначені;

– виявлення і реєстрація фактів порушення цілісності КЗЗ;

– інші події, обов'язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і

аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від НСД, модифікації або руйнування.

Одиночна ідентифікація та автентифікація (НИ-2)

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до захищених об'єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на нижчезазначені об'єкти і забезпечує їх взаємодію .

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені. Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

КЗЗ повинен забезпечувати захист даних автентифікації від НСД, модифікації або руйнування.

Однонаправлений достовірний канал (НК-1)

Послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з ЛОМ не може бути модифікованою іншим користувачем або процесом. Послуга повинна визначати вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об'єктів.

Достовірний канал повинен використовуватися для початкової ідентифікації та автентифікації. Зв'язок із використанням даного каналу повинен ініціюватися виключно користувачем.

Розподіл обов'язків адміністраторів (НО-2)

Послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів із певними й притаманними для кожної з категорій функціями. Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів й обмеження авторитарності керування АС.

Політика розподілу обов'язків, що реалізується КЗЗ, поширюється на користувачів усіх категорій і повинна визначати щонайменше такі ролі:

– адміністратора безпеки;

– не менше, ніж одного іншого адміністратора (адміністратора баз даних, адміністратора мережевого обладнання, адміністратора сервісів та ін.);

– користувачів, яким надано право доступу до конфіденційної інформації.

Ролі адміністраторів можуть дублюватися уповноваженими на це користувачами. Кількість таких користувачів повинна бути мінімальною.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального ПЗ, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління автоматизованої системи та системного й функціонального ПЗ, яке реалізує ці функції. Усім іншим користувачам доступ до цих об'єктів повинен бути заборонений.

Повинен заборонятися доступ адміністраторів до сильно- та слабозв'язаних об'єктів, що містять конфіденційну інформацію, за виключенням випадків, коли їхніми функціональними обов'язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки конфіденційної інформації.

КЗЗ з гарантованою цілісністю (НЦ-2)

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування при старті (НТ-2)

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій ЛОМ, що забезпечуються захистом.

Політика самотестування поширюється на нижчезазначені об'єкти і забезпечує їх взаємодію:

– адміністратора безпеки;

– компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ;

– засоби захисту інформації, а також технологічну інформацію КСЗІ.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в ЛОМ всіх критичних для безпеки конфіденційної інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, в якому забороняється обробка конфіденційної інформації взагалі, або до стану, в якому забороняється обробка конфіденційної інформації з використанням послуг безпеки, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

Автентифікація вузла (НВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, таких як цифровий підпис і коди автентифікації повідомлень. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

1.5 Висновок і постановка задачі

У першому розділі описаний об'єкт: рід діяльності, інформаційна система, інформаційні потоки, устаткування, програмне забезпечення. У технічному завданні виконаний, аналіз структури ІТС, аналіз загальної моделі погроз, визначений перелік порушників, інформаційних потоків і існуючих проблем у системі безпеки. Виконано вибір профілю захищеності підприємства.

В результаті проведеного обстеження ОІД побудовано модель загроз, що діють на дану ІТС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня інформаційної безпеки. Отримані результати будуть використані для розробки ПБ ІТС «Вектра».

нен стиль структуры: Двухбайтові
десь

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Політика інформаційної безпеки

Інформація, процеси, що її підтримують, інформаційні системи та сітьова інфраструктура, які є істотними активами сучасних фірм, підприємств та організацій, все частіше зштовхуються із різними загрозами безпеки,

такими як комп'ютерне шахрайство, шпіонаж, шкідництво, вандалізм. Тому актуальною є задача інформаційного захисту підприємств. Наявність політики інформаційної безпеки свідчить про зрілість та компетентність підприємства у питаннях забезпечення інформаційної безпеки.

В роботі розглядається вирішення задачі розробки політики інформаційної безпеки, яка б регламентувала та регулювала процеси доступу, зберігання та обробки інформації на підприємстві.

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства. У документі політики безпеки рекомендовано вносити наступні розділи :

– Вступний розділ, що підтверджує стурбованість керівництва проблемами інформаційної безпеки.

– Організаційний розділ, що описує підрозділи, комісії, групи осіб, відповідальні за роботи в області інформаційної безпеки.

– Класифікаційний розділ, що описує матеріальні та інформаційні ресурси підприємства та необхідний рівень їх захисту.

– Штатний розділ, що характеризує заходи безпеки щодо персоналу.

– Розділ, що висвітлює питання фізичного захисту інформації.

– Розділ управління, що описує підхід до управління комп'ютерами та комп'ютерними мережами пересилання даних.

– Розділ, що зазначає правила розмежування доступу до інформації.

– Розділ, що описує заходи, спрямовані на забезпечення безперервної роботи підприємства (доступності інформації).

Ефективна політика інформаційної безпеки визначає необхідний та достатній набір вимог безпеки. Вона мінімально впливає на продуктивність

праці, враховує особливості бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається й виконується співробітниками підприємства.

Інформаційними ресурсами, що підлягають захисту є: стандарти підприємства, електронні бази даних , договори та робочі документи.

Вимоги політики безпеки поширюються на всю інформацію і ресурси обробки інформації підприємства. Дотримання Політики обов'язкове для всіх співробітників, як постійних, так і тимчасових. У договорах з третіми особами, одержуючи доступ до інформації компанії, має бути обумовлений обов'язок третьої особи по дотриманню вимог Політики.

2.1.2 Організаційні заходи щодо забезпечення ПБ

1) розробити та впровадити посадові інструкції користувачів та персоналу ІТС, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;

2) обмежити доступ в приміщення, в яких відбувається обробка та зберігати інформації з обмеженим доступом згідно матриці доступу;

3) розробити та впровадити розпорядчі документи щодо правил перепусткового режиму на територію, де розташована ІТС;

4) розробити та впровадити розпорядчі документи щодо використання робочих станцій користувачами та зазначити в них що користувач несе матеріальну відповідальність за цілісність робочої станції;

5) визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації, яка обробляється на ОІД згідно матриці доступу;

6) створити на програмному рівні системи розпізнавання й розмежування доступу до інформації засобами ідентифікації й автентифікації користувачів даної ІТС;

7) розмежувати права користувачів ІТС у групи користувачів, згідно з матрицею доступу, програмними методами ОС;

8) блокувати облікові записи користувачів після певного числа невдалих спроб входу в систему, що зменшить вірогідність підбору паролю неавторизованим користувачем за допомогою функції менеджера облікових записів, до якої входить підтримка механізму ідентифікації і перевірки дійсності користувачів при вході в систему, блокувати ПЕОМ на час відсутності користувача;

9) створити набір прав, що дозволяє надавати користувачеві доступ на виконання окремих операцій та використання окремих програм за допомогою програмного продукту DeviceLock;

10) організувати захист атрибутами файлів. При цьому передбачена можливість встановлювати, чи може індивідуальний файл бути змінений або розділений визначеним користувачем. Захист атрибутами файлів використовується для запобігання випадкових змін або видалення окремих файлів. При захисті даних використовуються файлові атрибути: «модифікація, читання, копіювання, друкування, знищення» програмними засобами;

11) контролювати доступ користувачів до CD-і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB- портів за допомогою програмного продукту DeviceLock, чим забезпечиться мінімізація занесення вірусу з боку зовнішніх носіїв та зменшиться вірогідність копіювання інформації;

12) знищувати інформацію (або створити резервну копію), що зберігається в ПЗУ, при списанні або відправці ПЕВМ в ремонт;

13) захищати локальні розділи диску від випадкового або навмисного форматування;

14) ідентифікувати зовнішні носії на які здійснюється архівування даних, ідентифікувати периферійні засоби вводу\виводу інформації (клавіатури, миші, принтери), надаючи користувачеві доступ до пристрою з

відповідним ідентифікатором (драйвером або серійним номером) програмним методом;

15) протоколювати всі дії користувачів з пристроями і файлами згідно матриці доступу (копіювання, читання, знищення і т.п);

16) встановити нове антивірусне програмне забезпечення та налаштування між сітьового екрану;

17) зберігати конфіденційну інформацію на окремому спеціально виділеному локальному диску та обмежити до нього мережевий доступ програмними засобами.

18) обмежувати доступ до соціальних мереж та засобів миттєвого обміну повідомленнями, а також до сайтів, які не зв'язані з робочим процесом програмними засобами;

19) заборонити користувачам скачування та встановлення будь-яких програм програмними засобами;

20) налаштувати поштовий антивірусний монітор, який скануватиме кожне повідомлення і доставить на ящик листи які не містять ні вбудованого шкідливого коду, не інфікованих вкладень ;

21) заблокувати невживані порти комутатора програмними засобами.

22) роздати обов'язки системних адміністраторів програмними засобами.

23) при виникненні необхідності обміну даними через незахищене середовище налаштувати міжмережевого екрану на використання тільки протоколів SSL та IPsec, а також використання електронного цифрового підпису для забезпечення цілісності документів, що передаватимуться через незахищений канал зв'язку.

2.2 Розроблення елементів ПБ

2.2.1 Політика безпеки відносно паролів

Мета політики безпеки:

Встановити правила використання паролів для до баз даних, електронних документів, а також використання паролів для підключення до безпровідної мережі підприємства. Користувачі системи повинні дотримуватися вимог, що висвітлюються даній політиці. Виконання вимог даної політики відносно паролів підвищує рівень захищеності інформаційних ресурсів, що циркулюють та обробляються на підприємстві.

Область дії:

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ до баз даних чи електронних документів чи підключаються до АС підприємства за допомогою безпровідної мережі.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики паролів користувачами системи є заступником директора .

Політика безпеки:

Паролі системного рівня:

– паролі видаються заступником директора особисто, відповідальність за видачу паролів згідно приведеним нижче критеріям несе заступник директора.

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

а) латинські заголовні букви (A-Z);

б) латинські прописні букви (a-z);

в) цифри (0-9);

г) символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 3 місяці (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– паролі не мають повторюватися принаймні 3 рази.

Паролі рівня користувачів:

– паролі генеруються користувачами особисто та вони мають відповідно приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

а) латинські заголовні букви (A-Z);

б) латинські прописні букви (a-z);

в) цифри (0-9);

г) символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім'я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– паролі не мають повторюватися принаймні 3 рази.

Паролі для доступу до безпровідної мережі:

– паролі генеруються користувачами особисто та вони мають відповідно приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

а) латинські заголовні букви (A-Z);

б) латинські прописні букви (a-z);

в) цифри (0-9);

г) символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім'я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– паролі не мають повторюватися принаймні 3 рази.

Затвердження політики:

Політика безпеки розробляється заступником директора та підписується директорам закладу при прийнятті усіх розділів політики.

Дії з виконання політики інформаційної безпеки:

Виконання політики безпеки контролює системний адміністратор підприємства за допомогою вбудованих засобів аутентифікації в ОС. При прийнятті (зміні) політики безпеки кожен співробітник має бути ознайомлений не пізніше, чим за 5 робочих днів до прийняття нової редакції даної політики. При ознайомленні з даною політики безпеки користувач має підписатися, що він ознайомлений з нею, та зобов'язується виконувати встановлені цим документом правила.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз у рік заступником директора. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів. До співробітників, що порушили дану політику безпеки, будуть прийняті дисциплінарні міри.

2.2.2 Політика забезпечення доступу до серверу закладу

Мета політики безпеки:

Встановити правила та порядок доступу до серверів та у серверне приміщення. Дотримання вимог даної політики підвищую захищеність інформації, що зберігається та обробляється на сервері.

Область дії:

Дана політика розповсюджується на системних адміністраторів та заступника директора.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики доступу до серверів є заступник директора.

Політика безпеки:

Право доступу до серверної кімнати та знаходження у ньому без нагляду мають системний адміністратор та заступник директора, ключі від приміщення мають також системний адміністратор та заступник директора.

Право доступу до серверної кімнати під наглядом системного адміністратора чи заступника директора надається тільки співробітникам підприємства, що мають доступ до АС.

Доступ до апаратної частини серверів має системний адміністратор під наглядом заступника директора. Доступ надається при:

– проведенні профілактичних робіт;

– ремонті обладнання;

– заміни комплектуючих;

– модернізації апаратної частини.

Порядок доступу до апаратної частини:

– на ім'я заступника директору оформлюється заява на відкриття серверу з зазначенням мети доступу;

– після прийняття заяви, при наявності заступника директора знімається пломби системного адміністратора та заступника директора;

– під наглядом заступника директора системний адміністратор виконує необхідний обсяг роботи;

– по закінченні роботи встановлюються пломби системного адміністратора та заступника директора;

– оформлюється звіт з зазначенням початку(з моменту зняття пломб) до закінчення (встановлення нових пломб) із зазначення виду та обсягу проведених робіт.

Логічний доступ (віддалений доступ з використанням свого облікового запису) системний адміністратор використовує для настройки, проведення профілактичних робіт, інсталяція чи видалення програмного забезпечення, усунення несправністей, модернізація ПО, оновлення антивірусних баз. Доступ реалізується засобами видаленого адміністрування з необхідними для авторизації системного адміністратора даних зі свого робочого місця.

Логічний доступ користувачів виконується віддалено з їх робочих станцій. Згідно з їх правами доступу.

Логічний доступ заступник директора виконує віддалено з його робочого місця для аналізу захищеного журналу та перевірки працездатності КЗЗ.

Затвердження політики:

Політика безпеки розробляється заступником директора та директором при прийнятті усіх розділів політики.

Дії з виконання політики інформаційної безпеки:

Виконання політики безпеки користувачами контролює системний адміністратор підприємства за допомогою вбудованих засобів аудиту в ОС. Виконання політики безпеки користувачами, в тому числі й системним адміністратором контролюється заступником директора за допомогою вбудованих засобів аудиту в ОС. При прийнятті (зміні) політики безпеки кожен співробітник має бути ознайомлений не пізніше, чим за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз у рік заступником директора. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

Системний адміністратор та заступник директора несуть відповідальність за виконання політики доступу до серверу та серверного приміщення.

2.2.3 Політика використання Інтернет на підприємстві

1 Мета

Підвищити рівень інформаційної безпеки компанії шляхом введення правил і інструкцій для співробітників, які при виконанні своїх прямих обов'язків використовують Інтернет.

2 Зона дії

Політика поширюється на співробітників закладу, які при виконанні своїх прямих обов'язків використовують Інтернет. Дана політика безпеки не відміняє інші політики.

3 Затвердження політики

Політика використання Інтернет була розроблена заступником директора і системним адміністратором.

До початку впровадження політики всі співробітники підприємства були ознайомлені з текстом даної політики (під розпис). Затвердження політики безпеки було виконано директором закладу організації.

4 Історія документа

Дана політика безпеки складається вперше на цьому підприємстві для підвищення рівня інформаційної безпеки.

5 Положення політики

Правила, описані в цій політиці, відносяться для всіх співробітників, які при виконанні своїх прямих обов'язків використовують Інтернет.

5.1 Доступ до Інтернет виконувати лише через устаткування і системи підприємства.

5.2 Використання Інтернет можливо лише для:

– підтримки і розвитку бізнесу і комунікації співробітників фірми;

– досліджень і розробок;

– збору інформації для більшої обізнаності у виробничих, фінансових, законодавчих питаннях, якщо ці питання безпосередньо впливають на виконання своїх посадових обов'язків;

5.3Забороняється:

– грати на комп'ютері в робочий час і під час обіду;

– вести діяльність не від імені фірми;

– передавати конфіденційну інформацію на сторону;

– здійснювати дії що перечать статуту ділової етики підприємства, законодавству, політикам і процедурам підприємства;

– доступ до неавторизованої інформації і її копіювання;

– доступ до системи під іншим паролем.

Використання електронної пошти, дошок оголошень, чат-кімнат в робочий час, на устаткуванні фірми і застосовуючи імена користувачів і паролі фірми в особистих цілях, для переговорів з друзями і членами сім'ї розглядається як експлуатація ресурсів компанії в особистих цілях і категорично забороняється. Жодних виключень не робиться з даного питання для обідніх перерв і неробочого часу.

6 Відповідальність

У разі явного порушення даної політики співробітником підприємства, він буде негайно усунений від використання Інтернет, а інформація про це буде зафіксована в особистому файлі співробітника.

7 Виключення

В даній політиці безпеки немає виключень, всі описані випадки використання є оптимальними.

8 Порядок і періодичність перегляду

Політика безпеки передивляється з періодичністю разів в 6 місяців. Після публікації нової або зміни існуючої політики безпеці компанії, кожен співробітник, який використовує Інтернет для виконання своїх прямих обов'язків, повинен підписатися в угоді про обов'язковість виконання вимог даної політики.

2.2.4 Політика антивірусного захисту

1 Мета

Підвищити інформаційну безпеку компанії шляхом розробки системної політики по створенню, впровадженню і супроводу комплексних засобів антивірусного захисту, які визначають основні правила і вимоги по захисту інформаційних ресурсів організації від загроз, пов'язаних з дією програм, спеціально розроблених або модифікованих для несанкціонованого знищення, блокування, зміни або копіювання інформації, а також порушення нормального процесу функціонування організації.

2 Зона дії

Політика поширюється на всіх співробітників закладу, які в своїй професійній діяльності використовують комп'ютери, і є обов'язковою для виконання. Дана політика безпеки не відміняє інші політики.

3 Затвердження політики

Політика використання Інтернет була розроблена заступником директора і системним адміністратором. До початку впровадження політики всі співробітники підприємства були ознайомлені з текстом даної політики (під розпис). Затвердження політики безпеки було виконано директором Шахти.

4 Історія документа

Дана політика безпеки складається вперше на цьому закладі для підвищення рівня інформаційної безпеки.

5 Політика

5.1 Засоби захисту від шкідливих програм мають бути встановлені, налагоджені і активізовані на всіх програмно-технічних засобах до початку їх використання для роботи з інформаційними ресурсами організації.

До використання допускаються лише ліцензійні антивірусні засоби, рекомендовані до використання системним адміністратором. У разі потреби використання антивірусних засобів, що не увійшли до переліку рекомендованих, їх вживання необхідно погоджувати з системним адміністратором.

Установка засобів антивірусного захисту на комп'ютерах і налаштування їх параметрів здійснюється системним адміністратором відповідно до керівництва по вживанню конкретних антивірусних засобів.

5.2 Контролю на предмет виявлення шкідливих програм повинна піддаватися вся інформація, що створюється або обробляється програмно-технічними засобами, а також інформація, що приймається або передається по знімних носіях і засобам телекомунікації.

5.3 Оновлення антивірусних баз повинне виконуватися не рідше одного разу на добу автоматично, згідно з можливостями програмного забезпечення. В разі збою автоматичного оновлення, оновлення баз виконується уручну з тією ж періодичністю системним адміністратором.

5.4 Заходи щодо антивірусного захисту включають:

5.4.1 Профілактику вірусів :

1) щоденна автоматична перевірка наявності вірусів при включенні комп'ютера;

2) регулярна (не рідше за один раз в квартал) вибіркова перевірка комп'ютерів на наявність вірусів, навіть за відсутності зовнішніх проявів вірусів. При виявленні вірусів на комп'ютері, що працює в локальній мережі, перевірці підлягають всі комп'ютери, включені в цю мережу і працюючі із загальними даними і програмним забезпеченням;

3) перевірка наявності вірусів в комп'ютерах, що повернулися з ремонту (у тому числі гарантійного);

4) створення резервної копії програмного продукту відразу ж після придбання;

5) ретельна перевірка всіх програм, що поступають, а також куплених програм і баз даних;

6) обмеження доступу до комп'ютера сторонніх осіб.

5.4.2 Аналіз ситуацій

1) якщо антивірусні програми видають на екран дисплея повідомлення про підозріння на наявність вірусів на комп'ютері, то перш за все необхідно переконатися в дійсній наявності вірусів. Можливі ситуації, при яких ці повідомлення є наслідком несправності комп'ютера.

2) при виникненні подібної ситуації необхідно припинити роботу і негайно сповістити системного адміністратора, а також суміжні підрозділи, що використовують ці файли в роботі.

3) якщо вірус проник на комп'ютер із знімного носія, то необхідно визначити джерело і, якщо джерело інформації на знімному носієві знаходиться в організації, то необхідно перевірити на наявність вірусів комп'ютер – джерело інформації на знімному носієві. Якщо джерело дискети або знімного носія – комерційна або інша організація, то необхідно повідомити в цю організацію про факт виявлення вірусів і надалі звернути особливу увагу на носії інформації, що поступають з цієї організації.

5.4.3 Вживання засобів антивірусного захисту

1) якщо вірус уразив які-небудь програми, то знищення вірусу виконується шляхом знищення програми на диску, або на дискеті. Після знищення зараженої програми необхідно відновити програму, використовуючи резервну копію програми.

2) якщо вірус уразив файли, то вірус знищується, або шляхом стирання цих файлів, або шляхом використання спеціальних програм, що лікують. Використання програм, що лікують, не дає повної гарантії відновлення файлу. Тому після лікування необхідна перевірка відновлення даного файлу. Програми, що лікують, використовуються лише в тих випадках, коли відсутня

резервна копія зараженої програми або файлу з даними, або відновлення знищеного файлу за допомогою резервної копії дуже трудомістко.

3) після знищення вірусів і відновлення заражених програм і файлів з даними необхідно ще раз виконати перевірку наявності вірусів, використовуючи антивірусні програми. Перед повторною перевіркою необхідно перезавантажити комп'ютер через виключення і подальше включення комп'ютера.

6 Вимоги до співробітників

– співробітники зобов'язані проводити антивірусний контроль всіх зовнішніх носіїв інформації;

– у всіх випадках можливого прояву дії вірусів, виявлення файлів, уражених вірусом або підозри на наявність вірусу співробітники повинні:

а) без спроби якого-небудь лікування негайно повідомити про це системному адміністраторові і оцінити з ним можливі шляхи зараження і поширення даного вірусу;

б) спільно з системним адміністратором провести лікувально-відновні заходи.

– співробітники зобов'язані робити резервні копії файлів, що містять коштовну службову інформацію;

– співробітники не повинні самостійно встановлювати програмне забезпечення, якщо це не входить в їх обов'язки. Забороняється встановлювати і запускати неліцензійне програмне забезпечення або таке, що не відноситься до виконання посадових обов'язків;

– заборонене використання знімних носіїв, що належать особам, тимчасово допущеним до роботи на комп'ютері (студенти-практиканти, що тимчасово заміщають, співробітники сторонніх організацій тощо).

7 Відповідальність:

– відповідальність за виконання заходів антивірусного контролю і дотримання вимог даної політики покладається на всіх співробітників закладу, що є користувачами системи;

– відповідальність за проведення профілактичних заходів щодо забезпечення антивірусного захисту, а також знищення виявлених вірусів покладається на системного адміністратора;

– періодичний контроль за станом антивірусного захисту, а також за дотриманням встановленого порядку антивірусного контролю і виконанням вимог даної політики співробітниками здійснюється системним адміністратором.

8 Виключення

Усі виключення з політики мають бути погоджені з директором. Неузгоджені відступи від політики розцінюються як інциденти інформаційної безпеки і можуть служити підставою для прийняття адміністративних заходів відповідно до законодавства.

9 Порядок і періодичність перегляду

Політика антивірусного захисту передивляється з періодичністю раз на півроку. При виникненні частих ситуацій, що порушують інформаційну безпеку підприємства, періодичність перегляду політики може змінюватися.

Після внесення змін до політики безпеки кожен співробітник закладу має бути ознайомлений з новою версією політики і підписатися в угоді про обов'язковість виконання вимог даної політики.

2.2.5 Інструкція з використання електронної пошти

1 Електронна пошта надається працівникам компанії тільки для виконання своїх службових обов'язків. Використання її в особистих цілях заборонено.

2 Розмір поштової скриньки користувача обмежений 5 Гб. У разі перевищення зазначеного ліміту прийом кореспонденції для користувача припиняється до моменту появи вільного місця в поштовій скриньці.

3 Електронна пошта використовується для обміну службовою інформацією у вигляді текстових повідомлень або документів в електронному вигляді.

4 Діють наступні правила для блокування вихідної кореспонденції: блокуються вихідні і вхідні електронні повідомлення наступного вигляду:

– повідомлення без теми;

– повідомлення, одночасно адресовані більше 5 кореспондентам;

– повідомлення, що містять вкладені файли наступних форматів:

– виконувані файли (розширення -. Exe,. Dll,. Pif тощо);

– мультимедіа файли (аудіо та відео);

– повідомлення, що містять більше 3 вкладених файлів;

– повідомлення розміром понад 10 Мб.

5 Для зменшення розміру електронних повідомлень і об'єднання декількох вкладених файлів в один рекомендується використовувати програми для стиснення (компресії) вкладених документів (WinRar).

Користувачам ЗАБОРОНЯЄТЬСЯ:

– використовувати корпоративну електронну пошту в особистих цілях;

– робити розсилання матеріалів рекламного (непрофільного) і розважального характеру;

– виробляти масову розсилку листів невиробничого характеру;

– пересилати виконувані файли (з розширеннями -. Exe,. Dll,. Pif тощо);

– пересилати мультимедійні файли (аудіо та відео);

– робити розсилання шкідливих програм або файлів, заражених вірусами;

– використовувати електронну пошту для передачі матеріалів великого обсягу (більше 10 Мб);

– використання безкоштовних поштових сервісів Інтернет (mail.ru, yandex.ru, і т.д.);

– публікувати свій корпоративний адресу, або адреси інших працівників компанії на загальнодоступних Інтернет ресурсах (форуми, конференції тощо);

– здійснювати масову розсилку поштових повідомлень рекламного характеру без попереднього узгодження з співробітниками Служби ІТ;

– надавати, кому б-то не було пароль доступу до своєї поштової скриньки;

– пересилати по поштою паролі до яких би то не було ресурсів компанії.

6 Користувачам надається право відправки електронної пошти зовнішнім абонентам, які є працівниками компанії, на підставі заявки підписаної керівником структурного підрозділу.

7 Користувачам забороняється відправка в незахищеному вигляді електронних повідомлень, що містять комерційну таємницю. Інформацію про способи захисту повідомлень можна отримати в службі ІТ.

8 Вся вихідна пошта, що відправляється зовнішнім абонентам, які є працівниками компанії, архівується і контролюється на предмет наявності інформації, що становить комерційну таємницю.

2.3 ВИСНОВОК

В спеціальній частині було розроблено сукупність правил, відносно паролів, доступ до сервера, використання інтернету, антивірусний захист і використання електронної пошти на підприємстві, які повинні сприяти забезпеченню політики безпеки інформаційно-комунікаційних системи концерну "Вектра"

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є визначення економічної доцільності використання запропонованих засобів та заходів інформаційної безпеки на ТОВ «Вектра».

Для визначення цього необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити обсяги відвернених втрат, та, на основі цього, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі розрахованих показників можна буде визначити, наскільки прибутковим або збитковим є запропонований проект.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.[6]

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної;
– витрати на залучення зовнішніх консультантів;
– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);
– вартість створення основного й додаткового програмного забезпечення (ПЗ);
– витрати на первісні закупівлі апаратного забезпечення;
– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);
– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Відповідно до специфіки розробленої ПБ та конкретних рішень, обраних у цій політиці, актуальними капітальними витратами можна вважати наступні:

– вартість розробки проекту інформаційної безпеки;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Трудомісткість у даному випадку буде розраховуватися за формулою 3.1:

$$t = t_{об} + t_{а} + t_{вз} + t_{озб} + t_{д\,год}, \qquad (3.1)$$

де $t_{об}$ – тривалість проведення обстеження АС підприємства; $t_{а}$ – 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; $t_{д}$ – тривалість документального оформлення політики безпеки.

Показники часу, витраченого на розробку політики інформаційної безпеки наведені у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	Значення, год
$t_{об}$	65
$t_{а}$	16
$t_{вз}$	10
$t_{озб}$	16
$t_{д}$	16

Згідно з формулою 3.1 трудомісткість розробки ПБ становить:

$$t = 65\,год + 16\,год + 10\,год + 16\,год + 16\,год,$$

і, таким чином,

$$t = 123\,год.$$

Надалі потрібно розрахувати витрати на створення ПБ ($K_{рп}$), використовуючи наступні показники – витрати на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) та вартість витрат машинного часу ($З_{мч}$). Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп}\,грн. \qquad (3.2)$$

У свою чергу, витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб},\,грн, \qquad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин; $З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, в загальному випадку, становить – 72 грн/год.

Згідно з формулою 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 123\,год \cdot 72\,грн/год,$$

і, таким чином,

$$З_{зп} = 8856\,грн.$$

Тож, витрати на створення ПБ за формулою 3.2 становлять:

$$K_{рп} = 8856\ грн.$$

У результаті розрахунків, маємо вартість розробки ПБ – 8*856* гривень.

У даному конкретному випадку повна вартість капітальних витрат розраховується за формулою 3.4:

$$K = K_{рп} + K_{навч}\ грн. \qquad (3.4)$$

Під $K_{навч}$, мається на увазі одноразовий кваліфікаційний захід для співробітників, з питань ознайомлення з новою редакцією політики безпеки. Даний захід проводиться спеціалістом ІБ, тому додатково йому виплачується сума у розмірі 500 грн, окрім виплати за розробку нової редакції ПБ.

Тож, згідно до формули 3.4, повна вартість капітальних витрат становить:

$$K = 8856\ грн + 500\ грн,$$

і, таким чином,

$$K = 9356\ грн.$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.[6]

Для даного підприємства актуальними будуть наступні витрати:

– заробітна плата обслуговуючого персоналу;
– кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки;
– технічне й організаційне адміністрування й сервіс.

Оскільки методи захисту, передбачені політикою безпеки, мають більш організаційний характер, поточними витратами можна вважати заробітну платню системного адміністратора, витрати на опечатування зовнішніх

інтерфейсів робочих станцій та витрати пов'язані з діяльністю користувачів, тож поточні витрати розраховуються за формулою 3.5:

$$C = C_{за} + C_{оп} + C_{дк}\ грн, \qquad (3.5)$$

де $C_{за}$ – витрати на заробітну плату системного адміністратора; $C_{оп}$ – витрати на опечатування зовнішніх інтерфейсів робочих станцій; $C_{дк}$ – витрати, пов'язані з діяльністю користувачів.

У свою чергу, витрати на заробітну плату системного адміністратора розраховуються за формулою 3.6:

$$C_{знад} = З_{дод1} + З_{дод2}\ грн, \qquad (3.6)$$

Де $З_{дод1}$ – додаткова заробітна плата системного адміністратора за проведення кваліфікаційних заходів та перевірку знать та навичок персоналу стосовно правил, регламентованих політикою безпеки; $З_{дод1}$ – додаткова заробітна плата системного адміністратора за додаткові обов'язки – відповідальність за виконання деяких розділів політики безпеки інформації.

Додаткова заробітна платня №1 складає 500 грн за проведення одного кваліфікаційного заходу. Такі заходи планується проводити раз на 2 місяці, тож фактично за місяць системний адміністратор отримуватиме 250 грн додаткової заробітної платні №1 на місяць. Додаткова платня №2 враховуватиме обсяг відповідальності, що покладатиметься на системного адміністратора політикою безпеки. Таким чином, розмір додаткові заробітної платні №2 становитиме – 1000 грн/місяць.

За формулою 3.6, можна розрахувати:

$$C_{знад} = (250\ грн\ + 1000\ грн) \cdot 12\ місяців,$$

і, таким чином,

$$C_{знад} = 15000\ грн.$$

Поточні витрати за опечатування зовнішніх інтерфейсів на рік включатимуть у себе вартість 2 журналів (200 грн) опечатування та 150 пломб-наліпок (450 грн). Тож:

$$C_{оп} = 200\ грн + 450\ грн,$$

і, таким чином,

$$C_{оп} = 650\ грн.$$

Витрати, пов'язані з діяльністю користувачів мають під собою на увазі витрати, що спричинені професійною діяльністю. Такою діяльністю вважається перенавантаження серверу і частий перезапис інформації на жорстких дисках серверу у процесі роботи, що приведе сервер у неробочий стан. Такі витрати включають у себе вартість полагодження серверу, профілактична заміна компонентів. За рік, вартість таких витрат сягатиме 1500 грн. Тож:

$$C_{дк} = 1500\ грн.$$

Розрахунок повної вартості експлуатаційних витрат за формулою 3.5:

$$C = 15000\ грн + 650\ грн + 1500\ грн,$$

і, таким чином,

$$C = 17150\ грн.$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Далі буде вказано загрози з можливим економічним впливом на підприємство:

1 злам мережі, порушення нормального функціонування системи призводить до простою на підприємстві;
2 несанкціоноване ознайомлення з інформацією (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати

частини запланованого заробітку через використання цих даних конкурентами;

3 несанкціонована модифікація/видалення інформації (співробітниками) призведе до порушення робочого процесу, що у свою чергу призведе до втрати частини запланованого заробітку;

4 несанкціоноване копіювання інформації на знімні носії (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

5 помилки персоналу, що дозволяють зловмисникам отримати доступ до системи мають схожий ефект зі зламом мережі;

6 несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками має схожий ефект з несанкціонованим ознайомленням з інформацією працівниками;

7 несанкціонована модифікація/видалення інформації конкурентами та зловмисниками має схожий ефект з несанкціонованою модифікацією/видаленням інформації співробітниками;

8 крадіжка/псування матеріальних цінностей (об'єктів ІТС) конкурентами та зловмисниками призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

9 використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами має схожий ефект зі зламом мережі;

10 злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди має схожий ефект зі зламом мережі;

11 збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює, у свою чергу це призведе

до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

12 відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи, що в свою чергу призведе до втрати частини запланованого заробітку.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V \text{ грн}, \tag{3.7}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн; $П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн; V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ і V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс}{F} \cdot t_п \text{ грн}, \tag{3.8}$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн}, \tag{3.9}$$

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.

$$V = \frac{О}{F} \cdot (t_п + t_в + t_{ви}) \text{ грн}, \tag{3.10}$$

де F – місячний фонд робочого часу; O – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \ грн, \qquad 3.11$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \ грн, \qquad 3.12$$

де F – місячний фонд робочого часу; $З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

Відповідно до пронумерованого вище списку загроз, можна розрахувати ймовірні збитки. Враховуючи той факт, що деякі загрози мають схожі наслідки, розрахунки будуть проводитись для одного випадку з групи подібних, але надалі буде враховуватись кількість можливих подій на рік та ймовірність їх виникнення.

Відповідно до переліку загроз, вказаного вище, для загроз №1, №5, №9, №10 збитки від реалізації однієї з цих загроз розраховуються за формулами 3.7–3.11:

$$П_п = 13000\ грн \cdot 14\ чол/212\ год \cdot 3\ год,$$

$$П_п = 2575{,}47\ грн.$$

$$П_{ви} = 0\ грн.$$

$$П_{зч} = 0\ грн.$$

$$П_{пв} = 14000\ грн/212\ год \cdot 1\ год,$$

$$П_в = 66{,}03\ грн.$$

$$П_в = 0\ грн + 66{,}03\ грн + 0\ грн,$$

$$П_в = 66{,}03\ грн.$$

$$V = 3001065\ грн/212\ год \cdot (3\ год + 1\ год + 0\ год),$$

$$V = 56623{,}86\ грн.$$

І таким чином,

$$U = 2575{,}47\ грн + 66{,}03\ грн + 56623{,}86\ грн,$$

$$U = 59264{,}5\ грн.$$

Тобто, збиток від одноразової реалізації загроз №1, №5, №9 або №10 становитиме – 59264 грн 50 копійок.

Для загроз №2, №4, №6 потрібно враховувати не збитки, а розмір не одержаної вигоди від реалізації однієї з цих загроз. Експертним висновком розмір неодержаної вигоди визначені у розмірі – 90031,95 грн/місяць (3% від планового місячного прибутку підприємство не буде отримувати).

Оскільки загрози №8 та №12 мають схожі наслідки, розмір збитку від реалізації однієї з загроз буде таким самим і для іншої і буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000\ грн/212\ год \cdot 24\ год,$$

$$П_п = 1471{,}70\ грн.$$

$$П_{ви} = 0 \text{ грн.}$$

Враховуючи специфіку роботи підприємства, одним з найцінніших ресурсів компанії є робочі станції (ноутбуки), тому в якості показника $П_{зч}$ враховується вартість заміни ноутбука.

$$П_{зч} = 8000 \text{ грн.}$$

$$П_{пв} = 14000 \text{ грн}/212 \text{ год} \cdot 120 \text{ год},$$

$$П_{в} = 7924{,}52 \text{ грн.}$$

$$П_{в} = 0 \text{ грн} + 7924{,}52 \text{ грн} + 8000 \text{ грн},$$

$$П_{в} = 15924{,}52 \text{ грн.}$$

$$V = 1478 \text{ грн}/212 \text{ год} \cdot (120 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 823{,}58 \text{ грн.}$$

І таким чином,

$$U = 1471{,}70 \text{ грн} + 15924{,}52 \text{ грн} + 823{,}58 \text{ грн},$$

$$U = 18219{,}8 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загрози №8 становитиме – 18219 грн 80 копійок.

Оскільки загроз № 3, № 7 та №11 мають подібні наслідки, збиток від їх реалізації буде розраховуватись за формулами 3.7–3.11:

$$П_{п} = 13000 \text{ грн} \cdot 14 \text{ чол}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_{п} = 2575{,}47 \text{ грн.}$$

$$П_{ви} = 14000 \text{ грн}/212 \text{ год} \cdot 3 \text{ год},$$

$$П_{ви} = 198{,}11 \text{ грн.}$$

$$П_{зч} = 0 \text{ грн.}$$

$$П_{пв} = 0 \text{ грн.}$$

$$П_{в} = 198,11 \text{ грн} + 0 \text{ грн} + 0 \text{ грн},$$

$$П_{в} = 198,11 \text{ грн.}$$

$$V = 3001065 \text{ грн}/212 \text{ год} \cdot (3 \text{ год} + 3 \text{ год} + 0 \text{ год}),$$

$$V = 84935,80 \text{ грн.}$$

І таким чином,

$$U = 2575,47 \text{ грн} + 198,11 \text{ грн} + 84935,80 \text{ грн},$$

$$U = 87709,30 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз № 3, № 7 або №11 становитиме – 87709 грн 30 копійок.

Таким чином, маючи дані про можливі збитки від реалізації загроз можна провести розрахунок збитків на рік від реалізації даних загроз. Зводні дані та кінцева величина збитку зазначені у таблиці 3.2:

Таблиця 3.2 – Розрахунок річних обсягів збитків від реалізації загроз

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Злам мережі, порушення нормального функціонування системи	59264,5	1	0,54	32002,83

Продовження таблиці 3.2

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Несанкціоноване ознайомлення з інформацією (співробітниками)	90031,95	1	0,3	27009,59
Несанкціонована модифікація/видалення інформації (співробітниками)	87709,30	2	0,3	52625,58
Несанкціоноване копіювання інформації на знімні носії (співробітниками)	90031,95	1	0,32	28810,22
Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи	59264,5	1	0,70	41485,15
Несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками	90031,95	1	0,5	45015,98
Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди	59264,5	1	0,72	42670,44
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює	87709,30	1	0,36	31575,35

Продовження таблиці 3.2

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи	18219,8	1	0,36	6559,13
ЗАГАЛЮМ				372581.72

Для розрахунку коефіцієнтів вірогідності були використані дані з таблиць 1.8 і 1.9, а саме – коефіцієнти К2, що відповідають за мотивацію джерела загрози і зручність використання вразливості відповідно. Рівні коефіцієнта К2 були відповідно змінені на часткову шкалу (1 – 0,2; 2 – 0,4; 3 – 0,6; 4 – 0,8; 5 – 1). На підставі коефіцієнтів К2 джерела і коефіцієнтів К2 вразливості експертним шляхом були визначені коефіцієнти вірогідності реалізації зазначених вище загроз.

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою :

$$E = B \cdot R - C \text{ грн}, \qquad (3.13)$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн; R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці; C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Тож, економічний ефект становить:

$$E = 372581{,}72 \text{ грн} - 17150 \text{ грн},$$

$$E = 355431 \text{ грн}.$$

В загальному вигляді, оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій $T_О$.

У даному випадку ТСО не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.14:

$$ROSI = E / K, \qquad (3.14)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн; К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Тож,

$$ROSI = 372581{,}72 \text{ грн} / 9356 \text{ грн},$$

$$ROSI = 39{,}8.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $Е_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.15:

$$ROSI > (N_{деп} - N_{інф}) / 100 \qquad (3.15)$$

де $N_{деп}$ = 19 – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %; $N_{інф}$ = 8 – річний рівень інфляції, %.

39,8 > 0,11, отже проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.16:

$$T_o = E / K = 1 / ROSI = 0,025 \text{ року.} \qquad (3.16)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки капітальних та поточних витрат на введення та експлуатацію засобів захисту, що рекомендовані політикою безпеки.

В ході розрахунків було з'ясовано що введення в експлуатацію засобів та заходів захисту є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (0,025 року), а коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта (39,8 > 0,11). Тож, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВОК

Під час виконання кваліфікаційної роботи було виконано обстеження об'єкта інформаційної діяльності відповідно до порядку обстеження, описаному в НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Окрім цього було проведена класифікація інформації що циркулює в ІТС ТОВ «Вектра» та яка підлягає захисту. Класифікація проводилась відповідно до положень ЗУ «Про інформацію», якими регламентується перелік інформації що може, або не може бути інформацією з обмеженим доступом.

Після визначення вхідних даних, була проведена класифікація існуючих в ІТС загроз та їх джерел, шляхом експертної оцінки з використанням рекомендацій, описаних у документі ISO/IEC TR 13335-3:1998. Окрім цього було визначено клас автоматизованої системи (відповідно до НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу») та оцінено існуючий стан захищеності, шляхом аналізу існуючого функціонального профілю, а також розроблено новий функціональний профіль (відповідно до НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»), що відповідає вимогам, необхідним для запобігання інцидентів ІБ.

На основі отриманих даних був розроблений комплекс рекомендацій, щодо підвищення стану захищеності ІТС ТОВ «Вектра». Доцільність використання даних рекомендацій, в свою чергу, була обґрунтована у економічній частині кваліфікаційної роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1 Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: закон України редакції від 19.04.2014 № 1170-VII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр

2 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]: НД ТЗІ 3.7-003-05 від "8" листопада 2005 №125. – Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

3 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-004-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/

4 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-005-99 від 07.01.1999. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/

5 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 1.1-002-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/

6 Експлуатацію систем інформаційної безпеки [Електронний ресурс] – Режим доступу: https://lektsii.org/15-1904.html

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	36	
6	А4	Розділ 2. Спеціальна частина	18	
7	А4	Розділ 3. Економічна частина	16	
8	А4	Висновок	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

- Горянський С.В. 125-17-1.docx
- Горянський С.В. 125-17-1.pptx

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. ВІДГУК КЕРІВНИКА ДИПЛОМНОЇ РОБОТИ

«Розробка політики безпеки інформації інформаційно-комунікаційних системи ТОВ "Вектра"»

студента групи 125-17-1 Горянського Станіслава Владиславовича

Дипломний проект за спеціальністю 125 «Кібербезпека» Горянського С.В представлена пояснювальною запискою на 85 стор., містить 2 рис., 13 табл., 4 додатка, 6 джерела.

Мета дипломної роботи – підвищення інформаційної безпеки підприємств, де кінцевий користувач має доступ і обробляє інформацію у в комп'ютерній корпоративної мережі. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання дипломного проекту були вирішені наступні питання: аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для ОІД ТОВ "Вектра", приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

До недоліків проекту слід віднести окремі невідповідності вимогам оформленні та не чітко розкрито аналіз ризиків.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до дипломного проекту спеціаліста і заслуговує оцінки "добре", а Горянському Станіславу Владиславовичу присвоєння кваліфікації "професіонал з управління інформаційною безпекою" освітньо-кваліфікаційного рівня "спеціаліст".

.

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.