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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студентки *Рябчинської Варвари Костянтинівни*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «МонтажЕнерго»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корченко А.В.			
розділів:				
спеціальний	ас. Олішевський І.Г.			
економічний	к. е. н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студентці ***Рябчинській В.К.*** **академічної групи** ***125-20-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «МонтажЕнерго»***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

Розділ	Зміст	Термін виконання
1	Стан питання, розробка моделі загроз і моделі порушника, постановка задачі.	26.05.2024
2	Розробка політики безпеки інформації, визначення профілю захищеності, проєктні рішення.	19.06.2024
3	Розрахунок річних витрат на розробку політики безпеки, оцінка величини збитку. Розрахунок ефективності.	26.06.2024

Завдання видано _____ Корченко А.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Рябчинська В.К.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 83 сторінки, 2 рисунки, 8 таблиць, 7 додатків, 10 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи ТОВ «МонтажЕнерго».

Мета кваліфікаційної роботи: підвищити рівень інформаційної безпеки ІКС ТОВ «МонтажЕнерго».

У розділі «Стан питання. Постановка задачі» виконаний аналіз об'єкту інформаційної діяльності ТОВ «МонтажЕнерго», розглянуто атаки інформаційних систем та засоби аналізу захищеності мереж підприємства. Проведено обстеження об'єкта, розроблена модель загроз, модель порушника, сформульовано задачі проєкту.

У розділі «Спеціальна частина» був розглянутий функціональний профіль захищеності та розроблені проєктні рішення щодо забезпечення безпеки ІКС ТОВ «МонтажЕнерго».

В економічному розділі визначається економічна ефективність заходів, що впроваджуються, призначених для захисту інформації в ТОВ «МонтажЕнерго».

Практична цінність кваліфікаційної роботи полягає в підвищенні рівня безпеки інформації з обмеженим доступом ТОВ «МонтажЕнерго» шляхом впровадження політики безпеки.

Розроблена політика безпеки призначена для впровадження та використання в ТОВ «МонтажЕнерго» з метою захисту інформації.

ПОЛІТИКА БЕЗПЕКИ, КОМЕРЦІЙНА ТАЄМНИЦЯ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ІКС.

ABSTRACT

The explanatory note consists of 83 pages, 2 images, 8 tables, 7 appendices, 10 sources.

Object of development: the information security policy of the information and communication system of MontazhEnergo LLC.

Purpose of qualification work: to increase the level of information security of the information and communication system (ICS) of MontazhEnergo LLC.

In the section "Status of the issue. Statement of the problem" it is performed an analysis of the object of information activity of MontazhEnergo LLC, it is considered attacks on information systems and tools for analyzing the security of the company's networks. An inspection of the object was carried out, a threat model, a model of the violator was developed, and project tasks were formulated.

In the "Special part" section, the functional security profile was considered and project solutions were developed to ensure the security of ICS of MontazhEnergo LLC.

The economic section determines the economic efficiency of the implemented measures designed to protect information at MontazhEnergo LLC.

The practical value of the qualification work is to increase the level of security of information with limited access of MontazhEnergo LLC by implementing a security policy.

The developed security policy is intended for implementation and use in MontazhEnergo LLC for the purpose of information protection.

SECURITY POLICY, COMMERCIAL SECRET, UNAUTHORIZED ACCESS, ICS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДКР – дослідно-конструкторська робота;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

КЗЗ – комплекс засобів захисту від несанкціонованого доступу;

МКС – мережа комп'ютерної системи;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС – обчислювальна система;

ПЗ – програмне забезпечення;

ПРД – правила розмежування доступу;

СЗІ – служба захисту інформації;

ТЗ – технічне завдання.

ЗМІСТ

ВСТУП

Перед сучасними підприємствами гостро постають проблеми забезпечення інформаційної безпеки. Це пов'язане з розвитком інформатизації підприємства, з постійно зростаючою конкуренцією і, як наслідок, зростанням вартості інформації. Інформація, яка складає комерційну таємницю, може використовуватися компаніями-конкурентами, шахраями у своїх корисливих цілях, наносячи при цьому значний матеріальний або моральний збиток репутації підприємства - власникові цієї інформації.

На сучасному підприємстві порушення ІБ спричиняє порушення бізнес-процесів, втрату доходів, зниження довіри інвесторів і клієнтів, погіршення репутації, втрату даних, правові наслідки, тощо.

Рішення питань організації захисту інформації на підприємстві шляхом впровадження сучасних захищених інформаційних технологій і надійних засобів захисту інформації є рішенням важливого практичного завдання керівництвом підприємства й відповідних підрозділів безпеки. Адекватний рівень інформаційної безпеки в організації може бути забезпечений тільки на основі комплексного підходу, що припускає використання як програмно-технічних, так і організаційних мір захисту.

Питання забезпечення безпеки інформаційного простору в організації здобувають все більшу актуальність. З розвитком інформаційних технологій з'являється усе більше погроз функціонування ІКС, що спричиняє, як результат, поліпшення й розвиток технічних і програмних засобів протидії порушенням безпеки інформаційного середовища.

У цей час питання забезпечення безпечного інформаційного простору виносяться в організаціях різного типу на перший план, забезпечення конфіденційності даних є невід'ємною частиною успішного функціонування організації в сфері своєї діяльності.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ТОВ «МонтажЕнерго»

Товариство з обмеженою відповідальністю «МонтажЕнерго» займається будівельно–монтажними роботами.

Підприємство розташоване на другому поверсі чотирьохповерхового будинку в орендованому приміщенні за адресою: м. Кам'янське, вул. Українська 10.

На підприємстві встановлений п'ятиденний робочий тиждень.

Графік роботи – з 9.00 до 18.00, Пн-Пт, з перервою на обід з 13.00 до 14.00.

Штат співробітників офісу підприємства складається з 9 чоловік:

- директор – 1 особа;
- заступник директора – 1 особа;
- бухгалтер – 1 особа;
- техніки – 5 осіб;
- системний адміністратор – 1 особа.

Існуюча на підприємстві інформація:

- податкова інформація, архів звітів;
- база даних нормативних документів, форми та бланки договорів;
- фінансова інформація, квитанції та чеки, розписки;
- база даних договорів про надання послуг, виконання робіт; документи, що регулюють механізми співробітництва з іншими підприємствами, документи, що затверджують право підприємства займатися підприємницькою діяльністю;
- база даних об'єктів;
- база даних клієнтів;
- архів копій договорів надання послуг, виконаних робіт, протоколів засідань, довідок та інша архівна та статистична інформація;
- інформація о співробітниках, керівництві;
- ілюстрації, фотоматеріали, презентації.

1.2 Загальні положення політики безпеки

Під політикою безпеки інформації слід розуміти набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою тощо. Політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування.

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;

– достатності механізмів і заходів захисту та їхньої адекватності загрозам;

– гнучкості керування системою захисту, простоти і зручності її використання;

– відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна доказово давати гарантії того, що:

– в АС забезпечується адекватність рівня захисту інформації рівню її критичності;

– реалізація заходів захисту інформації є рентабельною;

– в будь-якому середовищі функціонування АС забезпечується оцінюваність і перевірюваність захищеності інформації;

– забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів АС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування АС;

– персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

– всі критичні з точки зору безпеки інформації технології (функції) АС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

– враховані вимоги всіх документів, які регламентують порядок захисту інформації в АС (п. 6 додатку), та забезпечується їхнє суворе дотримання.

Політика безпеки розробляється на підготовчому етапі (НД ТЗІ 3.7-001-99) створення КСЗІ. Методологія розроблення політики безпеки включає в себе наступні роботи:

– розробка концепції безпеки інформації в АС;

– аналіз ризиків;

– визначення вимог до заходів, методів та засобів захисту;

– вибір основних рішень з забезпечення безпеки інформації;

– організація виконання відновлювальних робіт і забезпечення неперервного функціонування АС;

– документальне оформлення політики безпеки.

Концепція безпеки інформації в АС викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної АС і виконується на підставі аналізу наступних чинників:

– правових і (або) договірних засад;

– вимог до забезпечення безпеки інформації згідно з завданнями;

– загроз, яким зазнають впливу ресурси АС, що підлягають захисту.

За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в АС:

– мета і пріоритети, яких необхідно дотримуватись в АС під час забезпечення безпеки інформації;

– загальні напрями діяльності, необхідні для досягнення цієї мети;

– аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;

– відповідальність посадових осіб та інших суб'єктів взаємовідносин в АС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі.

Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об'єкти захисту). Для цього використовуються відомості п.3 додатку, одержані в результаті обстеження середовищ функціонування АС.

Встановлюється відповідність моделі загроз і об'єктів захисту, тобто

складається матриця загрози/компоненти (ресурси) АС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АС. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною

шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

– досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в АС;

– досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в АС;

– досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в АС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проєктування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм “ефективність/вартість”), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється. Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

Вихідними даними є:

– завдання і функції АС;

– результати аналізу середовищ функціонування АС;

– модель загроз, модель порушників;

– результати аналізу ризиків.

На підставі цих даних визначаються компоненти АС (наприклад, окрема ЛВС, спеціалізований АРМ, Internet-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в АС.

Для кожного компонента та (або) АС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99). Визначені вимоги складають профіль захищеності інформації в АС (компоненті).

Для кожного компонента та (або) АС в цілому визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

Комплекс заходів з забезпечення безпеки інформації розглядається на трьох рівнях:

– правовому;

– організаційному;

– технічному.

На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– системи нормативно-правового забезпечення робіт з захисту інформації в АС (організації);

– підтримки керівництвом організації заходів з забезпечення безпеки інформації в АС (організації), виконання правових та (або) договірних вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ;

– процедур доведення до персоналу і користувачів АС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань

безпеки інформації;

– системи контролю за своєчасністю, ефективністю і повнотою реалізації в АС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– застосування режимних заходів на об'єктах АС;

– забезпечення фізичного захисту обладнання АС, носіїв інформації, інших ресурсів;

– організації проведення обстеження середовищ функціонування АС;

– порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб'єктами системи ТЗІ в Україні;

– виконання робіт з модернізації АС (окремих компонентів);

– регламентації доступу сторонніх користувачів до ресурсів АС;

– регламентації доступу власних користувачів і персоналу до ресурсів АС;

– здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

– реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до АС, використання мереж передачі даних загального користування).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

– інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти АС, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

– реєстрація санкціонованих користувачів АС, авторизація користувачів в системі;

– керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

– виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

– перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в АС;

– забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

– резервне копіювання критичних даних, супроводження архівів даних і ПЗ;

– відновлення роботи АС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;

– захист ПЗ, окремих компонентів і АС в цілому від внесення несанкціонованих доповнень і змін;

– забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Повинні бути вироблені підходи щодо планування і порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій (надзвичайних ситуацій) з метою забезпечення неперервного функціонування АС в захищеному режимі. Під час планування цих робіт рекомендується враховувати наступні питання:

– виявлення критичних з точки зору безпеки процесів у роботі АС;

– визначення можливого негативного впливу надзвичайних ситуацій на роботу АС;

– визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

– підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення відновлювальних робіт і забезпечення неперервного функціонування АС повинен описувати дії щодо улагодження інциденту, дії щодо резервування, дії щодо відновлення. Він включає в себе:

– опис типових надзвичайних ситуацій, які потенційно найбільш можливі в АС внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

– опис процедур реагування на надзвичайні ситуації, які слід вжити відразу після виникнення інциденту, що може призвести до порушення політики безпеки;

– опис процедур тимчасового переводу АС або окремих її компонентів на аварійний режим роботи;

– опис процедур поновлення нормальної виробничої діяльності АС або окремих її компонентів;

– порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

План проведення відновлювальних робіт і забезпечення неперервного функціонування АС підлягає перегляду у разі виникнення істотних змін в АС. Такими змінами можуть бути:

– встановлення нового обладнання або модернізація існуючого, включення до складу АС нових компонентів;

– встановлення нових систем життєзабезпечення АС (сигналізації, вентиляції, пожежогасіння, кондиціонування та ін.);

– проведення будівельно-ремонтних робіт;

– організаційні зміни у структурі АС, виробничих процесах, процедурах обслуговування АС;

– зміни у технології обробки інформації;

– зміни у програмному забезпеченні;

– будь-які зміни у складі і функціях КСЗІ.

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів АС, складають правила розмежування доступу (ПРД).

ПРД – це певним абстрактним механізмом, який виступає посередником при будь-яких взаємодіях об’єктів АС і є найбільш суттєвим елементом політики безпеки.

Як приклад, загальні ПРД можуть бути наступними (за припущення, що в АС визначено такі ієрархічні ролі – адміністратор безпеки АС, адміністратор, користувач):

– кожне робоче місце повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;

– для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів АС, керування механізмами захисту здійснюється адміністратором безпеки АС;

– для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання ПЗ несуть: на АРМ – користувачі, адміністратор, в АС – адміністратор безпеки АС. Використовуватись повинно тільки ПЗ, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

– за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки АС. Такі роботи виконуються за його дозволом;

– кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки АС. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

– користувачі проходять процедуру автентифікації для отримання доступу до ресурсів АС;

– атрибути користувачів періодично змінюються, а невикористовувані і скомпрометовані – видаляються;

– процедури використання активного мережевого обладнання, а також окремих видів ПЗ, яке може суттєво впливати на безпеку (аналізатори трафіку,

аналізатори безпеки мереж, засоби адміністрування та ін.), авторизовані і здійснюються під контролем адміністратора безпеки АС;

– усі користувачі повинні знати "Інструкцію користувача" (пройти відповідний курс навчання, скласти іспит);

– адміністратор безпеки АС і адміністратори повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з точки зору безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в АС. Структурно до політики безпеки (документів, що її складають) повинні входити наступні розділи:

– загальний, у якому визначається відношення керівництва АС (організації) до проблеми безпеки інформації;

– організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та ін.);

– класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в АС, та необхідний рівень їхнього захисту;

– розділ, у якому визначаються ПРД до інформації;

– розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

– розділ, у якому висвітлюються питання фізичного захисту;

– розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

– розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

– розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування АС;

– юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі», створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІКС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення КЗЗ здійснюється в усіх ІКС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІКС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.

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

Це ж стосується и розробки ПБ, як одного з етапів побудови КСЗІ.

1.3 Характеристики ОІД

Товариство з обмеженою відповідальністю «МонтажЕнерго» займається будівельне – монтажними роботами.

Підприємство розташоване на другому поверсі чотирьохповерхового будинку в орендованому приміщенні за адресою: м. Кам’янське, вул. Українська 10.

На підприємстві встановлений п'ятиденний робочий тиждень.

Графік роботи – з 9.00 до 18.00, Пн-Пт, з перервою на обід з 13.00 до 14.00.

Штат співробітників підприємства складається з 9 чоловік:

– директор – 1 особа;

– заступник директора – 1 особа;

– бухгалтер – 1 особа;

– техніки – 5 осіб;

– системний адміністратор – 1 чол.

Офіс, де розташовано підприємство, включає такі приміщення:

– кабінет директора;

– тамбур;

– кабінет 1(заст. директора, техніки);

– кабінет 2 (бухгалтер, системний адміністратор).

Фізичні характеристики будівлі і приміщень:

– зовнішні стіни а також стіна, що граничить з коридором – завтовшки 500мм, викладена з білої цегли;

– внутрішні стіни – завтовшки 150мм, викладені з білої цегли;

– підлога – залізобетонні плити перекриття, завтовшки 200мм, укриті лінолеумом;

– дах будівлі плоский, викладений руберойдом. Вихід на дах здійснюється через пожежні сходи;

– під дахом розташовано технічний поверх висотою 1,9 м;

– висота стелі у приміщеннях – 3 м;

– двері головного входу мають розміри 1200 мм х 2100 мм, виконані зі звареної листової сталі, оздоблені 3 механічними замками різних конструкцій; міжкімнатні двері мають розміри 900 мм*2100мм, виконані з ламінованого МДФ;

– на об'єкті є 4 вікна, розмірами 3000 мм х 1600 мм, виконані з 2-камерного розбірного дерев'яного профілю;

1.3.1 Характеристика систем, що функціонують в приміщенні

Приміщення підприємства обладнано:

– системами електропостачання, освітлення, телефонного зв'язку, опалення;

– живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж;

– телефонний зв'язок а також Інтернет ADSL здійснює «Укртелеком».

1.3.2 Характеристика ІКС

До складу ІКС входять 8 ПК під керуванням ОС Windows 11 та 1 Сервер під керуванням ОС Windows Server 2022. Встановлена антивірусна система – **ESET NOD32 Smart Security Business Edition**.

Схема ІКС наведена на рисунку 1.1.

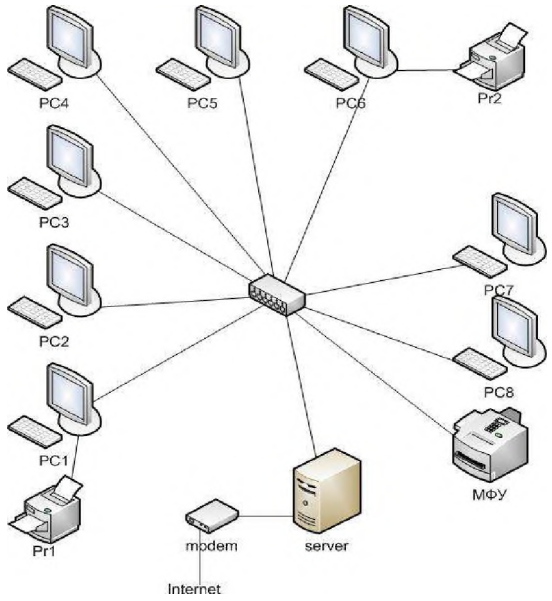

Рисунок 1.1 – Схема ІКС

Характеристика обладнання наведена в таблиці 1.1.

Таблиця 1.1 – Характеристика обладнання

Найменування	Модель, характеристики	Примітка
PC1	Intel Pentium G2020 (3M Cache, 2.90 GHz)/DDRIII/4096 Мб/HDD/500 Гб/Інтегрированний відеоадаптер/Intel HD Graphics/DVD±RW/	директор

Продовження таблиці 1.1

Найменування	Модель, характеристики	Примітка
PC2	Intel Pentium G2020 (3M Cache, 2.90 GHz)/DDRIII/4096 Мб/HDD/500 Гб/Інтегрований відеоадаптер/Intel HD Graphics/DVD±RW/	заступник директора
PC3 – PC5, PC7, PC8	Intel Pentium G2020 (3M Cache, 2.90 GHz)/DDRIII/4096 Мб/HDD/500 Гб/Інтегрований відеоадаптер/Intel HD Graphics/DVD±RW/	техніки
PC6	Intel Pentium G2020 (3M Cache, 2.90 GHz)/DDRIII/4096 Мб/HDD/500 Гб/Інтегрований відеоадаптер/Intel HD Graphics/DVD±RW/	бухгалтер
Server	Intel Core i5-3330 (6M Cache; 3.0 GHz)/DDRIII/4096 Мб/HDD/1000 Гб/Дискретний відеоадаптер/AMD Radeon HD7670 (1024Mb)/DVD±RW/Кардридер	системний адміністратор
Pr1	HP LJ Pro P1102	директор
Pr2	HP LJ Pro P1102	бухгалтер
МФУ	HP LJ Pro M1132	заступник директора, техніки
modem	TP-Link TD-8817	

1.3.3 Структура організації та обов'язки персоналу

Директор керує підприємством, спрямовує діяльність як підприємства в цілому, так і окремих працівників, відповідає за своєчасне та повне звітування перед відповідними контролюючими органами, консультує роботу техніків, супроводжує укладення договорів.

Заступник директора керує організаційною складовою діяльності підприємства, відповідає за рекламну кампанію організації, співпрацю з іншими підприємствами, організацію культурно-масових та професійних заходів. За відсутності директора виконує його обов'язки стосовно консультацій працівників та супроводження укладення договорів.

Бухгалтер відповідає за ведення всієї податкової та бухгалтерської документації, та формування звітної документації.

Техніки здійснюють пошук клієнтів, підбір об'єктів в Інтернеті, оголошення в газетах та в базах даних. Організовують виїзд на об'єкти, зустріч з замовником робіт, підготовку документів, консультує «проблемні» об'єкти, формують бази даних.

Системний адміністратор слідкує за правильною роботою ІКС та іншої техніки на підприємстві, за її своєчасним обслуговуванням та ремонтом або заміною, виконує підбір, купівлю, встановлення та налаштування компонентів ІКС та оргтехніки, проводить навчання основам комп'ютерної грамотності серед персоналу та консультацію з використання програмного забезпечення та оргтехніки.

1.3.4 Класифікація інформації, що циркулює в ІКС

Існуючу на підприємстві інформацію можна розділити наступним чином:

– податкова інформація, архів звітів;

– база даних нормативних документів, форми та бланки договорів;

– фінансова інформація, квитанції та чеки, розписки;

– база даних договорів про надання послуг, виконання робіт; документи, що регулюють механізми співробітництва з іншими підприємствами, документи,

що затверджують право підприємства займатися підприємницькою діяльністю;

– база даних об’єктів;

– база даних клієнтів;

– архів копій договорів надання послуг, виконаних робіт, протоколів засідань, довідок та інша архівна та статистична інформація;

– інформація о співробітниках, керівництві;

– ілюстрації, фотоматеріали, презентації.

Згідно цього можна класифікувати таку інформацію за ступенем значущості за трьома властивостями – доступністю, цілісністю та конфіденційністю.

Така класифікація приведена в таблиці 1.2.

Також інформацію можна класифікувати за типом (друковані дані, електронний текстовий документ, електронний графічний документ тощо) та розподілити за працівниками, що з нею працюють.

Така класифікація наведена в таблиці 1.3.

Таблиця 1.2 – Класифікація інформації

Властивість інформації	Ступінь значущості	Умовне позначення	Найменування інформації
1	2	3	4
Конфіденційність	Дуже важлива	К1	база даних об’єктів; база даних клієнтів;
	Важлива	К2	податкова інформація; фінансова інформація; база даних договорів; інформація о співробітниках, керівництві;

Продовження таблиці 1.2

1	2	3	4
	Корисна	К3	ілюстрації, фотоматеріали, презентації; архівна та статистична інформація; база даних оголошень; база даних бланків документів;
Цілісність	Критична	Ц0	база даних об'єктів; база даних клієнтів;
	Дуже важлива	Ц1	база даних бланків документів; фінансова інформація; база даних договорів;
	Важлива	Ц2	база даних оголошень; інформація о співробітниках, керівництві; податкова інформація;
	Корисна	Ц3	ілюстрації, фотоматеріали, презентації; архівна та статистична інформація;
Доступність	Критична	Д0	база даних об'єктів; база даних клієнтів;

Продовження таблиці 1.2

1	2	3	4
	Дуже важлива	Д1	база даних бланків документів; база даних оголошень;
	Важлива	Д2	податкова інформація; фінансова інформація; база даних договорів;
	Корисна	Д3	ілюстрації, фотоматеріали, презентації; архівна та статистична інформація; інформація о співробітниках, керівництві;

Таблиця 1.3 – Структура обробки та носії інформації

Інформація	Хто обробляє	Носій
1	2	3
база даних об’єктів	всі співробітники	електронний вигляд (текстові документи)
податкова інформація	директор, заступник директора, бухгалтер	друковані дані
база даних клієнтів	всі співробітники	друковані дані, електронний вигляд (текстові документи)

Продовження таблиці 1.3

1	2	3
інформація о співробітниках, керівництві	директор, заступник директора, бухгалтер	друковані дані, електронний вигляд (текстові документи)
база даних бланків документів	директор, заступник директора, бухгалтер	електронний вигляд (текстові документи)
архівна та статистична інформація	заступник директора, директор, бухгалтер	друковані дані, електронний вигляд (текстові документи)
ілюстрації, фотоматеріали, презентації	всі співробітники	електронний вигляд (графічні дані, презентації)
база даних договорів	директор, заступник директора, бухгалтер	друковані дані
фінансова інформація	директор, заступник директора, бухгалтер	друковані дані

1.4 Модель порушника

Порушником можуть бути наступні особи:

– співробітники підприємства;

– клієнти;

– персонал будівлі, де розташований об’єкт інформаційної діяльності, адміністрація;

– персонал, що обслуговує комунікації, які належать місту або приватним компаніям (наприклад, лінії телефонного зв’язку);

– керівники підприємства;

– відвідувачі, які знаходяться в межах КЗ по запрошенню з того чи іншого приводу;

– співробітники державних силових структур або органів, що контролюють діяльність підприємства (наприклад, інспектор податкової служби);

– технічний персонал підприємства або особи, що виконують встановлення, налаштування та оновлення ПЗ, що необхідне у зв'язку з напрямом діяльності підприємства.

Усіх порушників можна розділити на категорії відповідно до того, є вони співробітниками підприємства (внутрішні) чи сторонніх організацій (зовнішні), за їхніми мотивами, рівнем кваліфікації, та можливістю скоєння злочинних дій. Така класифікація приведена в таблиці 1.4.

Таблиця 1.4 – Модель порушника

Категорії порушників		Мотив	Кваліфікація	Можливість	$К_З^Д$
Внутрішні	Технічний персонал	1	5	4	0,16
	Співробітники	2	3	3	0,14
	Керівництво	1	2	5	0,08
Зовнішні	Клієнти, відвідувачі	1	2	1	0,02
	Обслуговуючий персонал будівлі, державні служби	2	3	2	0,10

У таблиці оцінювання груп порушників за кожною з трьох характеристик (мотив, кваліфікація, можливість) відбувається за наступними критеріями.

Мотив:

– 1 – відсутній мотив для вчинення злочинних дій;

– 2 – відсутній мотив, низький рівень відповідальності;

– 3 – самоствердження;

– 4 – матеріальна вигода;

– 5 – професійна діяльність.

Кваліфікація:

– 1 – не обізнаний зі структурою інформаційно-комунікаційної системи, відсутні навички виконання найпростіших дій з ПК;
– 2 – не обізнаний зі структурою інформаційно-комунікаційної системи, початковий користувач ПК;
– 3 – мінімальні знання про інформаційно-комунікаційну систему, початковий користувач ПК;
– 4 – добре обізнаний щодо структури ІКС, впевнений користувач ПК;
– 5 – докорінно знає структуру ІКС, найвищий рівень вмінь.

Можливість:

– 1 – є тимчасовий доступ у приміщення під наглядом;
– 2 – є тимчасовий доступ у приміщення та до ІКС під наглядом;
– 3 – є повний доступ у приміщення та до ІКС під наглядом у робочий час;
– 4 – є повний безконтрольний доступ до приміщення та ІКС у робочий час;
– 5 – повний безконтрольний доступ до приміщення та до ІКС будь-коли.

Коефіцієнт загрози $К_З$ обчислюємо за формулою (1.1):

$$К_З^Д = (\text{Мотив} \cdot \text{Кваліфікація} \cdot \text{Можливість}) / 125, \quad (1.1)$$

де 125 – максимально можливе значення добутку критеріїв.

1.5 Модель загроз

Для правильної постановки задачі по розробці комплексу мір на підприємстві необхідно скласти модель загроз, котра дасть чітке уявлення про те, які загрози найбільш ймовірні, за рахунок чого і реалізація яких загроз несе найбільшу небезпеку.

Ці заходи передбачають виявлення можливих джерел загроз, чинників, що роблять можливою реалізацію загрози і, як наслідок, дозволяють виділити найбільш актуальні загрози безпеки інформації.

1.5.1 Загрози

Серед загроз, що діють на інформацію на підприємстві можна перелічити такі:

– знищення;
– блокування;
– псування;
– викрадення.

1.5.2 Класифікація джерел загроз

Носіями загроз безпеці інформації є джерела загроз. Існує декілька класифікацій джерел. По-перше, розрізняють внутрішні (знаходяться всередині організації) та зовнішні (знаходяться за межами організації), адже методи боротьби с загрозою можуть розрізнятися в залежності від її типу.

Також розрізняють джерела, що існують внаслідок діяльності людини, або ті, що від неї не залежать.

За цими та іншими ознаками джерела поділяють на три основні групи:

– обумовлені діями суб'єкта (антропогенні);
– обумовлені використанням технічних засобів (техногенні);
– стихійні.

Антропогенні виникають внаслідок діяльності людини (суб'єкта) – навмисної чи ні. В цю групу входять цілеспрямовані дії по знищенню або викраденню інформації, а також дії, які через необережність або незнання призвели до втрати або псування інформації. Ця група є найрозповсюдженішою, вона добре піддається прогнозуванню та попередженню. До неї входять як внутрішні, так и зовнішні джерела.

Друга група складається з джерел загроз, які виникають внаслідок використання техніки. Загрози, пов'язані з втратою або псуванням інформації внаслідок виходу з ладу обладнання важко спрогнозувати и попередити, тому їм приділяють особливу увагу. Джерела цієї групи також можуть бути як зовнішніми, так и внутрішніми.

Остання група джерел представляє обставини, що мають непереборну силу и не піддаються попередженню. Найчастіше сюди відносять стихійні лиха та природні катаклізми, техногенні катастрофи, пожежі. Вони не піддаються прогнозуванню, тому заходи захисту від їх наслідків повинні виконуватися постійно. Як правило, таки джерела є зовнішніми по відношенню до об'єкта, що захищається.

Враховуючи вищезгадане, складемо такий перелік джерел загроз:

1 Антропогенні (в якості загроз цієї групи буде взято результат розрахунку моделі порушника);

2 Техногенні – внутрішні:

2.1 Технічні засоби обробки;

2.2 Програмне забезпечення;

2.3 Додаткові технічні засоби;

3 Техногенні – зовнішні:

3.1 Засоби зв'язку;

3.2 Інженерні комунікації;

4 Стихійні:

4.1 Пожежа;

4.2 Техногенні катастрофи.

Зведемо джерела в таблицю 1.5 і обчислимо коефіцієнти.

Таблиця 1.5 – Класифікація джерел загроз

Категорія			Відмово-стійкість	Фатальність	Цінність	$К_З^Д$
1			2	3	4	5
Техно-генні	Внутрі-шні	Технічні засоби обробки інформації	2	3	4	0,19

Продовження таблиці 1.5

1			2	3	4	5
		Програмне забезпе-чення	3	2	4	0,19
		Додаткові технічні засоби	4	2	3	0,19
	Зов-нішні	Засоби зв'язку	1	3	3	0,07
		Інженерні комуніка-ції	2	3	2	0,10
Стихійні		Пожежа	2	5	2	0,16
		Техноген-на катастрофа	1	4	2	0,06

У наведеній таблиці оцінювання груп джерел загроз за кожною з трьох характеристик (можливість, неусувність, особливості для стихійних джерел та відмовостійкість, фатальність та цінність для техногенних) відбувається за наступники критеріями.

Відмовостійкість:

– 1 – пристрій або система мають практично необмежений ресурс використання/ліцензійне програмне забезпечення з довгостроковою комерційною підтримкою;

– 2 – пристрій або система має конструктивно закладений великий ресурс, не потребує заміни витратних матеріалів/ліцензійне програмне забезпечення;

– 3 – пристрій або система піддається оперативному блоковому ремонту

шляхом заміни програмного забезпечення з відкритим кодом;

– 4 – пристрій або система має сильні механічні навантаження, потребує регулярної заміни витратних матеріалів/прикладне ПО від невідомого постачальника;

– 5 – пристрій або система працює в умовах надмірних, непередбачених конструкцією навантажень/тестові збірки та альфа-, бета-версії програмного забезпечення.

Фатальність:

– 1 – система або пристрій піддаються швидкій заміні або продубльовані/проблема вирішується перезапуском програми;

– 2 – система або пристрій піддаються швидкому ремонту/проблема вирішується перезапуском комп'ютера;

– 3 – система або пристрій потребують діагностики, після чого можуть бути відремонтовані шляхом купівлі або ремонту складових частин, що вийшли з ладу/проблема може бути вирішена лише адміністратором шляхом переналаштування;

– 4 – система або пристрій потребують діагностики у сервісному центрі, після чого можуть бути відремонтовані шляхом заміни складових частин або повної заміни/проблема може бути вирішена лише адміністратором шляхом перевстановлення;

– 5 – система або пристрій потребує повної заміни/проблема може бути вирішена лише сертифікованим фахівцем у спеціалізованому ПЗ.

Цінність:

– 1 – система або пристрій не мають впливу на роботу підприємства/сервісне ПЗ, підсистема налаштування графічного відображення;

– 2 – система або пристрій створюють комфортні умови для роботи/ПЗ, що використовується нечасто або може бути замінене;

– 3 – система або пристрій виконують допоміжні функції, що полегшують робочий процес/повсякденне ПЗ, що має встановлені аналоги;

– 4 – система або пристрій використовуються повсякденно для роботи/спеціалізоване ПЗ для роботи;

– 5 – система або пристрій забезпечують роботу всього підприємства/системне ПЗ.

Можливість:

– 1 – відсутні прояви такого джерела в минулому;

– 2 – прояви цього джерела або незначні, або відбуваються лише раз в декілька десятиріч;

– 3 – прояви такого джерела відбуваються нечасто

– 4 – відбуваються регулярно;

– 5 – відбуваються дуже часто.

Неусувність:

– 1 – прояв джерела не впливає на об'єкт;

– 2 – результат прояву можна швидко відновити з мінімальними для робочого процесу затратами;

– 3 – результат прояву джерела призводить до необхідності середніх затрат на відновлення та до тимчасового обмеження доступу до ресурсів, що захищаються;

– 4 – прояв джерела призводить до практично неусувних наслідків, що потребують великих затрат коштів та надовго обмежують доступ до інформації;

– 5 – неусувні наслідки: повне руйнування об'єкта та всього устаткування.

Особливості:

– 1 – об'єкт розташовано поза зоною дії природних катаклізмів та на ньому відсутні передумови виникнення стихійних джерел загроз;

– 2 – об'єкт розташовано поза зоною дії природних катаклізмів але на ньому присутні передумови виникнення стихійних джерел загроз;

– 3 – об'єкт розташовано в зоні дії природних катаклізмів, в якій протягом великого проміжку часу відсутні їх прояви, але на об'єкті присутні передумови виникнення стихійних джерел загроз;

– 4 – об’єкт розташовано в зоні, де багатолітні дослідження підтверджують виникнення катаклізмів;

– 5 – об’єкт розташовано в зоні, де висока ймовірність природних катаклізмів.

Коефіцієнт загрози $К_З^Д$ для стихійних джерел обчислюємо за формулою (1.2):

$$К_З^Д = (\text{Можливість} \cdot \text{Неусувність} \cdot \text{Особливості}) / 125, \quad (1.2)$$

де 125 – максимально можливе значення добутку критеріїв.

Коефіцієнт загрози $К_З^Д$ для техногенних джерел обчислюємо за формулою (1.3):

$$КЗ^Д = (\text{Відмовостійкість} \cdot \text{Фатальність} \cdot \text{Цінність}) / 125, \quad (1.3)$$

де 125 – максимально можливе значення добутку критеріїв.

1.5.3 Класифікація вразливостей

Загроза як можлива небезпека здійснення будь-якої дії, спрямованої проти об’єкта, що захищається, реалізується не сама собою, а через вразливості.

Вразливості є невід’ємними і обумовлені недоліками процесу функціонування, властивостями архітектури ІС, протоколами обміну та інтерфейсами, що застосовуються ПО та апаратними засобами, умовами експлуатації і місцем розташування.

Одній загрозі можна зіставити декілька вразливостей, ослаблення або повне усунення яких є одним з механізмів впливу на можливість реалізації загрози.

Розрізняють наступні класи вразливостей:

– об’єктивні;

– суб’єктивні;

– випадкові.

Об’єктивні вразливості витікають з особливостей побудови та технічних характеристик автоматизованої системі на об’єкті, що захищається. Їх неможливо повністю уникнути, проте вони можуть бути помітно послаблені.

Суб’єктивні вразливості залежать від дій людини і, в більшості випадків, усуваються організаційними та програмно-апаратними засобами.

Випадкові вразливості залежать від особливостей оточуючої середи та непередбачених обставин.

Враховуючи всі ці нюанси, зіставимо наступний перелік вразливостей:

Об’єктивні:

– відсутність системи резервування.

Суб’єктивні:

– помилки:

а) при експлуатації ПЗ;

б) при встановленні/настроюванні ПЗ;

в) при експлуатації апаратних засобів;

– порушення:

г) режиму доступу на територію підприємства та до технічних засобів ІКС;

г) режиму обробки і обміну інформацією;

д) режиму конфіденційності у неробочий час;

е) режиму обробки та обміну інформацією на друкованих носіях.

Випадкові:

– збій, відмова або пошкодження:

ж) технічних засобів, що обробляють інформацію;

з) додаткових технічних засобів;

и) програмного забезпечення;

к) електроживлення;

л) інженерних комунікацій.

Зведемо вразливості у таблицю 1.6 і вирахуємо коефіцієнт загрози для кожної вразливості.

Таблиця 1.6 – Класифікація вразливостей

Категорія		Фаталь-ність	Доступ-ність	Кіль-кість	$К_З^В$
Об’єктивні					
	Відсутність систем резервування інформації	5	2	4	0,32
Випадкові					
Збій, відмови або пошкодження:	Технічних засобів, що обробляють інформацію	3	1	3	0,07
	Додаткових технічних засобів	2	2	1	0,03
	Програмного забезпечення	3	3	3	0,22
	Електропостачання	3	1	1	0,02
	Інженерних комунікацій	2	1	1	0,02
Суб’єктивні					
Помилки	При експлуатації ПЗ	2	2	2	0,06
	При інсталюванні ПЗ	3	2	1	0,05
	При експлуатації апаратних засобів	2	2	2	0,06
Порушення	Режиму доступу на територію и до технічних засобів	3	1	1	0,02
	Режиму обробки і обміну інформацією	3	2	2	0,10
	Режиму конфіденційності у неробочий час	4	3	2	0,19
	Режиму обробки інформації на друкованих носіях	3	3	3	0,22

У наведеній вище таблиці оцінювання груп вразливостей за кожною з трьох характеристик (фатальність, доступність, кількість) відбувається шляхом виставлення оцінки рівня загрози для кожного з трьох критеріїв для кожної вразливості (1 – мінімальне значення, 5 – максимальне).

Обчислення коефіцієнта загрози $К_З^В$ відбувається за формулою (1.4):

$$К_З^В = \frac{\text{Фатальність} \cdot \text{Доступність} \cdot \text{Кількість}}{125}, \quad (1.4)$$

де 125 – максимально можливе значення добутку критеріїв.

На даному підприємстві не висуваються вимоги до захисту від витоку інформації технічними каналами.

1.5.4 Побудова моделі загроз

За результатами складення класифікацій джерел загроз та вразливостей, можна побудувати модель загроз (таблиця 1.7), яка ілюструє найбільш актуальні загрози, що діють на підприємстві, відкинувши ті, що мають коефіцієнт загроз нижче 0.01 як малоймовірні або незначні.

Коефіцієнт загрози $К_З^А$ вираховується як добуток коефіцієнтів $К_З^Д$ та $К_З^В$ відповідних джерела та вразливості.

Таблиця 1.7 – Модель загроз

Джерело	**Загроза**	**Вразливість**		**$К_З^А$**
1	2	3	4	5
Технічний персонал	Знищення, блокування, псування	Помилки	при експлуатації ПЗ	0,010
			при експлуатації апаратних засобів	0,010
Технічні засоби обробки інформації		Збій, відмова або пошкодження	технічних засобів, що обробляють інформацію	0,013

Продовження таблиці 1.7

1	2	3	4	5
Співробітники	Викрадення	Порушення	режиму доступу на територію підприємства та до технічних засобів	0,014
Співробітники	Знищення, блокування, псування		режиму обробки і обміну інформацією	0,014
Керівництво			режиму конфіденційності у неробочий час	0,015
Технічний персонал			режиму обробки і обміну інформацією	0,016
Керівництво			режиму обробки та обміну інформацією на друкованих носіях	0,018
Співробітники			режиму обробки та обміну інформацією на друкованих носіях	0,031
Програмне забезпечення	Псування, знищення	Збій, відмова або пошкодження	програмного забезпечення	0,042
Пожежа	Знищення	відсутність резервування	системи інформації	0,051

1.6 Постановка задачі

В результаті проведеного обстеження ОІД побудовано модель загроз, що діють на дану ІКС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня

інформаційної безпеки. Отримані результати будуть використані в наступній частині для розробки політики безпеки інформаційно-комунікаційної системи ТОВ «МонтажЕнерго».

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Функціональний профіль захищеності

Згідно з нормативними документами НД ТЗІ 2.5-005-99 та НД ТЗІ 2.5-004-99 оберемо підходящій профіль захищеності для ТОВ «МонтажЕнерго».

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту обчислювальної системи автоматизованої системи, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Інформаційно-комунікаційна система ТОВ «МонтажЕнерго» відноситься до автоматизованої системи класу 3, бо автоматизована система класу «3» — це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Згідно з цим обраний профіль для даного підприємства:

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 }

Більш докладно критерії цього профілю захищеності наведені в таблиці 2.1.

Таблиця 2.1 – Критерії функціонального профілю захищеності

№	Критерій	Опис критерію	Виконується в системі чи ні
1	2	3	4
1	КД-2 (Базова довірча конфіденційність)	В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.	Так
2	КО-1 (Повторне використання об'єктів)	КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта. Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення.	Так

Продовження таблиці 2.1

1	2	3	4
3	КВ-1 (Мінімальна конфіденційність при обміні)	Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації.	Так
4	ЦД-1 (Мінімальна довірча цілісність)	На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів)	Так
5	ЦО-1 (Обмежений відкат)	Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.	Так

Продовження таблиці 2.1

1	2	3	4
6	ЦВ-1 (Мінімальна цілісність при обміні)	Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівень ЦВ-1 даної послуги забезпечує мінімальний захист.	Так
7	ДР-1 (Квоти)	Послуга використання ресурсів дозволяє керувати використанням послуг і ресурсів користувачами. Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу.	Так
8	ДВ-1 (Ручне відновлення)	Дана послуга забезпечує повернення КС до відомого захищеного стану після переривання обслуговування. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.	Так
9	НР-2 (Захищений журнал)	Реєстрація дозволяє контролювати небезпечні для КС дії. Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням ПБ. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою авторизованих користувачів.	Так

Продовження таблиці 2.1

1	2	3	4
10	НИ-2 (Одиночна ідентифікація і автентифікація)	Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. За результатами ідентифікації і автентифікації користувача система (КЗЗ) приймає рішення про те, чи дозволено даному користувачеві ввійти в систему і використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача.	Так
11	НК-1 (Однонаправлений достовірний канал)	Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію.	Так
12	НО-2 (Розподіл обов'язків адміністраторів)	Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача. Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі специфічними наборами адміністративних обов'язків.	Ні

Продовження таблиці 2.1

1	2	3	4
13	НЦ-2 (КЗЗ з гаранто-ваною цілісніс-тю)	Дана послуга, цілісність комплексу засобів захисту, 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.	Так
14	НТ-2 (Само-тесту-вання при старті)	Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій комп'ютерної системи. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій.	Ні
15	НВ-1 (Автен-тифіка-ція вузла)	Послуга ідентифікація і автентифікація при обміні дозволяє одному КЗЗ ідентифікувати інший комплекс засобів захисту (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.	Так

2.1.1 Реалізація критеріїв профілю захищеності

КД-2 Базова довірча конфіденційність, реалізована в системі за допомогою служби каталогів ОС Windows – Active Directory.

КО-1 Повторне використання об'єктів, користувач після завершення роботи на комп'ютері вимикає його, і вся інформація про його діяльність не дістається наступному користувачеві. Це реалізовано ОС Windows.

КВ-1 Мінімальна конфіденційність при обміні, реалізована за допомогою відеонагляду за каналами передачі інформації, а також за носіями інформації. В ОС Windows ця послуга реалізується за допомогою крипто алгоритмів самої ОС Windows.

ЦД-1 Мінімальна довірча цілісність реалізована за допомогою розмежування прав доступу в ОС Windows.

ЦО-1 Обмежений відкат – дана послуга реалізується за допомогою вбудованої утиліти в ОС Windows.

ЦВ-1 Мінімальна цілісність при обміні – за допомогою хеш-функцій, контрольних сум, та цифрового підпису, які використовуються в ОС Windows.

ДР-1 Квоти – ця послуга реалізується за допомогою ОС Windows, котра дозволяє відстежувати, контролювати, використання дискового простору користувачами.

ДВ-1 Ручне відновлення – за допомогою засобів ОС Windows, тобто функції відновлення системи, яка дозволяє відновити системні файли і програми комп'ютера до того стану, при якому робота виконувалася правильно, і уникнути тривалого усунення несправностей.

НР-2 Захищений журнал – ця послуга реалізується веденням журналу в самій ОС Windows. Забезпечується реєстрацією подій, що підлягають аудиту, в трьох журналах аудиту – Журнал безпеки (Security Log), Журнал системи (System Log), Журнал застосувань (Application Log).

НИ-2 Одиночна ідентифікація і автентифікація – ця послуга реалізована ОС Windows, кожен користувач системи має свій логін та пароль. Неавторизований

користувач не має можливості без логіну та паролю увійти до системи. Для отримання інформації про користувача задіяна служба WinLogon та модуль Graphical Identification and Authentication (GINA).

НК-1 Однонаправлений достовірний канал – цей критерій реалізовано за допомогою спеціального криптографічного протоколу SSL 3.0, котрий забезпечує безпеку зв'язку.

НО-2 Розподіл обов'язків адміністраторів – ця послуга не реалізована.

НЦ-2 КЗЗ з гарантованою цілісністю – критерій реалізовано в системі за допомогою служби каталогів серверної ОС Windows. А точніше, за допомогою Active Directory – служби каталогів.

НТ-2 Самотестування при старті – ця послуга не реалізована.

НВ-1 Автентифікація вузла – реалізація критерію виконана за допомогою протоколу Kerberos, який забезпечує засоби взаємної перевірки стосовно дійсності клієнтів, наприклад, користувача, комп'ютера, служби або сервера. Завдяки підтримки протоколу Kerberos ОС надає користувачам можливість однократного введення автентифікаційних даних для доступу до всіх ресурсів і застосувань, до яких у них є права на доступ.

2.2 Проєктні рішення

2.2.1 План із забезпечення працездатності ІКС ТОВ «МонтажЕнерго»

1 Основна частина

1.1 Введення основних понять:

– апаратні засоби – це матеріальні об'єкти, використовувані в техніку;

– програмні засоби – це програми, а також засобу екранного й друкованого подання - користувальницький інтерфейс. Це нематеріальні об'єкти;

– технічні засоби включають апаратні й програмні засоби. У даному й документах, що додаються, розглядаються тільки засоби, що ставляться до комп'ютерів і мережі;

– ресурсами є логічні пристрої й інші структури подання даних для користувача;

– мережними ресурсами є ресурси доступні через мережу;

– локальними ресурсами є ресурси доступні безпосередньо на даному комп'ютері.

Там, де мова йде про групу, мається на увазі якась група користувачів, що спільно працює над якими-небудь документами. Така група може являти собою цілий відділ або підрозділ, або включати співробітників різних відділів і підрозділів.

1.2 Мета даного документа

Технічні засоби можуть надавати різний рівень захисту від несанкціонованого доступу й випадкових збоїв, а так само мати різні можливості. Завдання регламентування роботи з технічними засобами це встановлення правил роботи, що забезпечують ефективність,, необхідну безпеку й захист інформації з урахуванням цих фактів.

2 Загальний порядок роботи мережі

Системні адміністратори встановлюють правила роботи з інформацією, технічними засобами й правила використання ресурсів відповідно до можливостей, функціям, призначенню й ступеню захищеності цих засобів, ресурсів і вимогам до захисту й доступності інформації, з якої виробляються роботи.

Системні адміністратори визначають і вводять технічні засоби й ресурси, призначені для роботи з інформацією відповідно до вимог до захисту й доступності цієї інформації встановлюваними керівництвом.

Користувачі підкоряються правилам, установлюваним системними адміністраторами. Користувачі відповідальні за недотримання правил і як наслідок втрату й псую інформації, а також поширення її за межі, установлювані вимогами до захисту.

3 Правила роботи з технічними засобами

3.1 Користувачам забороняється самовільно робити складання, розбирання, установку й технічне обслуговування апаратних засобів, так само як установку, видалення, настроювання й декомпіляцію програмних засобів.

3.2 Користувачам забороняється запускати й використовувати програмні засоби крім засобів установлених і настроєних відділом програмного забезпечення або під його контролем.

3.3 Користувачам забороняється захист даних, способами не погодженими з адміністраторами, так само як знищення коштовних даних.

3.4 Користувачам забороняється зберігання даних у місцях не погоджених з адміністраторами.

3.5 Користувача зобов'язані виконувати процедури й обережності, запропоновані адміністраторами.

3.6 Користувачам забороняється розголошення інформації відкриваючий доступ інших осіб до технічних засобів і даним або передача засобів доступу до них.

3.7 Користувачам забороняється пошук засобів і шляхів ушкодження, знищення технічних засобів або подолання їхнього захисту, так само як використання таких засобів.

3.8 Користувачі зобов'язані повідомляти про всі виявлені випадки ушкодження або відмови технічних засобів і їхнього захисту у відділ програмного забезпечення.

3.9 Адміністратори зобов'язані розмежовувати права доступу відповідно до вимог до захисту й доступності інформації.

3.10 Адміністратори відповідальні за вибір засобів захисту й зобов'язані виставляти обмеження відповідно до їх можливостей.

3.11 Адміністратори повинні вчасно реагувати на повідомлення про відмови, ушкодження технічних засобів і їхнього захисту.

3.12 Адміністратори зобов'язані діяти в інтересах безпеки перш, ніж в інтересах зручності роботи користувачів.

3.13 Адміністратори й користувачі повинні дбайливо ставитися до технічних засобів.

4 Порядок парольного захисту

4.1 Роз'яснювальна частина

Обліковий запис користувача це його реквізити в мережі, основні параметри якої є ім'я й пароль користувача. Засобами керування обліковими записами всіх користувачів забезпечуються адміністратори мережі.

Права доступу в мережі розподіляються на основі облікових даних користувачів.

Пароль користувача, у випадку якщо він тримається в секреті, гарантує що:

– ніхто інший, не міг зробити дії, які були зафіксовані системою як дії даного користувача.

– ніхто не міг одержати доступ до інформації, що захищається, скориставшись обліковим записом користувача.

Якщо користувачеві потрібен доступ до даних іншого користувача, він може одержати його з відповідного дозволу, продовжуючи працювати під своїм обліковим записом.

Якщо користувачеві потрібні можливості, якими володіє комп'ютер іншого користувача, він може ввійти на ньому під своїм обліковим записом.

4.2 Нормативна частина

Користувач зобов'язаний зберігати свій пароль у таємниці й уводити його самостійно.

5 Правила роботи з обліковими записами:

– користувачам заводяться, відключаються облікові записи й з відповідні права за розпорядженням Генерального директора.

– облікові записи підлеглих можуть бути заблоковані на час відпустки за розпорядженням безпосереднього й будь-якого вищестоящого начальника, а так само відділу кадрів.

– обліковий запис підлеглого може бути тимчасово заблокована й розблокована, або змінене час доступу по ній через розпорядження начальника, якщо вона не була заблокована розпорядженням вищестоящого начальника.

– адміністратори зобов'язані записувати в журнал операції закладу, блокування, видалення облікових записів користувачів і груп.

6 Порядок роботи з документами

Користувач самостійно або його керівник визначають, чи є документ необхідним тільки користувачеві або іншим співробітникам і ступінь його конфіденційності. Якщо документ у наслідку необхідним іншим користувачам, він з бути поміщений у папку для групової роботи. Помістити документ в існуючу папку користувач може самостійно, а для створення нових групових папок варто звернутися до адміністраторів.

Поміщаючи документ у загальну папку, користувач дозволяє доступ до нього для всіх користувачів, що мають доступ до даної папки. Відправляючи документ по електронній пошті, користувач дозволяє доступ до документа тому одержувачеві, якому він його відправляє.

Особа, що дозволяє доступ до якого-небудь документа відповідає за можливе небажане відкриття інформації , яка містить в ньому тим особам, яким воно дозволяє доступ.

Правила роботи з документами й папками для документів:

– всі документи повинні зберігатися в особистих або загальних папках (паках для групової роботи) певних адміністраторами.

– доступ керівника до документів підлеглого дозволяється адміністраторами завжди.

– доступ користувача або групи до яких-небудь документів може бути дозволений тільки власником документів або керівником групи (відділу, підрозділу), що належать дані документи.

– документи, що мають відношення тільки до групи й потребуючого доступу з боку всіх членів групи, повинні зберігатися винятково в папці групи.

– папки для публікацій призначені для надання матеріалів групи (відділу, підрозділу) для загального використання, вони відкриті на читання для всіх, але на запис тільки для групи провідну дану папку.

7 Порядок роботи з базами даних

Права доступу до засобів і операцій роботи з базами даних, так само як і самі засоби, визначаються розроблювачами. Адміністратори й користувачі діють на підставі інструкцій і документації, складених розроблювачем.

Користувачі не мають права здійснювати самовільне копіювання й збереження баз даних.

8 Порядок роботи з електронною поштою

Всі користувачі, для забезпечення робочих потреб мають адресу і ящик електронної пошти. Користувачі повинні розуміти, що при відправленні й одержанні пошти через Інтернет, її конфіденційність не забезпечується. При обміні по електронній пошті діють наступні правила:

– користувачі повинні використовувати електронну пошту тільки для передачі повідомлень і документів, але не програм.

– адміністратори можуть висувати додаткові вимоги по вмісту повідомлень обумовлені міркуваннями сумісності форматів повідомлень і документів, що пересилаються по електронній пошті, як для внутрішнього, так і для зовнішнього обміну.

9 Порядок роботи з Інтернетом

9.1 Користувачі, забезпечені доступом в Інтернет, повинні використовувати його тільки для обміну інформацією, але не програмами.

9.2 Користувачі не повинні передавати закриту інформацію з каналів Інтернет.

9.3 Адміністратори надають доступ тільки до тих сервісам і адресам Інтернет, які є безпечними.

9.4 Користувачі не повинні ігнорувати попередження про можливе зниження рівня безпеки або небезпеки вмісту при передачі/одержанні інформації через Інтернет.

10 Нормативні засоби

При регламентуванні роботи в мережі враховуються обмеження технічних засобів, на які опирається робота мережі, і може бути використана термінологія розроблювачів даних технічних засобів з необхідними поясненнями. Додатково

до даного регламенту для з, систематизування й регламентування конкретних завдань відділом програмного забезпечення можуть уводитися й затверджуватися інструкції обов'язкові для виконання.

2.2.2 Інструкція із забезпечення працездатності ІКС

Справжня інструкція покликана гарантувати належне використання комп'ютерів і телекомунікаційних ресурсів співробітниками ТОВ «МонтажЕнерго» (надалі ОРГАНІЗАЦІЇ). Всі користувачі комп'ютерів зобов'язані використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись, правил етики й справжньої інструкції.

При недотриманні користувачами умов справжньої інструкції до них застосовуються адміністративні міри покарання, аж до звільнення, у відповідності зі ступенем провини, установленої службовим розслідуванням.

ОРГАНІЗАЦІЯ не відповідає за дії окремих користувачів, що порушили справжню інструкцію.

ОРГАНІЗАЦІЯ має право, перевіряти будь-який або весь аспекти комп'ютерної системи, у тому числі електронну пошту, щоб гарантувати дотримання цієї інструкції.

Співробітники не повинні розраховувати на конфіденційність інформації, що вони створюють, посилають або одержують за допомогою комп'ютерів.

Комп'ютерна й телекомунікаційна системи належать ОРГАНІЗАЦІЇ й можуть використовуватися тільки в робочих цілях.

1 Керівники структурних підрозділів повинні обґрунтувати необхідність виділення доступу в Internet і наявність електронної поштової скриньки (або декількох) на мережному робочому місці, визначити користувача, обмежити доступ іншим особам.

2 Керівники структурних підрозділів і користувачі повинні забезпечувати щоденний контроль перегляду й виїмки вхідної інформації.

3 Системний адміністратор, керівники структурних підрозділів і користувачі повинні забезпечувати строге дотримання мер безпеки з метою захисту корпоративної мережі від вірусів, що надходять по електронній пошті.

4 Керівники структурних підрозділів несуть службову відповідальність за вихідну інформацію, що направляється користувачами по електронній пошті іншим адресатам.

4.1 Вихідна інформація із приєднаною формою офіційного бланка й від імені керівника ОРГАНІЗАЦІЇ відправляється з обов'язковим збереженням у справі паперової копії, із присвоєнням обов'язкових реквізитів офіційного бланка.

4.2 Інформація, що направляється в рамках необхідного для роботи відділів і керувань інформаційного контакту з іншими організаціями, забезпечення нормального процесу надання послуг відправляється за узгодженням з керівником структурного підрозділу з дозволу керівництва ОРГАНІЗАЦІЇ.

4.3 Забороняється відсилання інформації особистого або комерційного характеру для рішення особистих проблем, а також інформації із прохання третіх осіб без узгодження з керівництвом ОРГАНІЗАЦІЇ.

4.4 Невірні, нав'язливі, непристойні, наклепницькі, образливі, загрозливі або протизаконні матеріали забороняється пересилати по електронній пошті або за допомогою інших засобів електронного зв'язку, а також відображати й зберігати на комп'ютерах. Користувачі, що помітили або одержали подібні матеріали, повинні відразу сповістити про це інциденті своєму керівникові.

4.5 Користувачі повинні ретельно продумувати зміст повідомлень електронної пошти й інших електронних документів, як якби це було письмове послання. Усе, що створено на комп'ютері може бути й, швидше за все, буде проаналізовано іншими співробітниками.

4.6 Мережний адміністратор або/і інша уповноважена особа здійснює систематичний і вибірковий контроль за інформацією минаючої через поштовий (інформаційний) сервер і при недотриманні інструкції користувачами інформує об цьому вищестояще керівництво.

5 Керівники структурних підрозділів забезпечують контроль цільового використання співробітниками ресурсів Internet.

5.1 Забороняється запит і одержання користувачами з Internet матеріалів розважального характеру (ігор, кліпів, і т.д.), крім випадків їхнього спеціального використання в службових цілях (тільки за узгодженням з керівництвом ОРГАНІЗАЦІЇ).

5.2 Забороняється запит і одержання користувачами з Internet програмних продуктів, крім випадків, пов'язаних з виробничою необхідністю. При цьому необхідно узгодження вищестоящого керівництва й забезпечення процесу технічним фахівцем.

6 Зберігання інформації в електронних папках користувачів на робочому місці здійснюється в наступному порядку:

6.1 Створюються папки для обміну файлами в мережі (інформація загального змісту).

6.2 Створюються папки з інформацією, що носить специфічний і конфіденційний характер. На дані папки користувачем і системним адміністратором установлюється спеціальний доступ.

7 При роботі в інформаційній комп'ютерній мережі заборонено:

7.1 Грати в комп'ютерні ігри.

7.2 Приносити різні комп'ютерні програми й намагатися встановити на локальний диск комп'ютера без повідомлення фахівців відділу інформації.

7.3 Перенастроювати програмне забезпечення комп'ютера, намагатися розібрати його.

7.4 Передавати, кому б те не був свій пароль.

7.5 Змінювати або копіювати файл, що належить іншому користувачеві, не одержавши попередньо дозволу власника файлу.

7.6 Можливість користувачів входити в інші комп'ютерні системи через мережу не дає їм права на підключення до цих систем і на їхнє використання, якщо на те не отримане спеціальний дозвіл з боку операторів цих систем.

8 Міри усунення несправності комп'ютерної техніки.

При виявленні різних несправностей у роботі комп'ютерної техніки або інформаційний комп’ютерній мережі ОРГАНІЗАЦІЇ, потрібно відправити заявку у відділ інформації.

2.2.3 Політика безпеки відносно паролів

Мета політики безпеки – встановити правила використання паролів 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 політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ до баз даних чи електронних документів.

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

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 20 днів (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– паролі не мають повторюватися принаймні 5 разів.

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) символи 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 30 днів (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 30 днів (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– паролі не мають повторюватися принаймні 3 рази.

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

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.

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

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

2.2.4 Інструкція з організації антивірусного захисту

Ця Інструкція визначає вимоги до організації захисту АС від руйнівного впливу комп'ютерних вірусів і встановлює відповідальність керівників і співробітників підрозділів, що експлуатують та супроводжуючих АС ТОВ «МонтажЕнерго», за їх виконання.

До використання в АС допускаються тільки ліцензійні антивірусні засоби, централізовано закуплені ТОВ «МонтажЕнерго» у розробників (постачальників) зазначених коштів.

Установка засобів антивірусного контролю на комп'ютерах (серверах АС) здійснюється уповноваженими співробітниками відділу інформаційних технологій. Налаштування параметрів засобів антивірусного контролю здійснюється співробітниками відділу інформаційних технологій відповідно до посібників по застосуванню конкретних антивірусних засобів.

1 Застосування засобів антивірусного контролю

Щодня на початку роботи при завантаженні комп'ютера (для серверів ІКС – при перезапуску) в автоматичному режимі повинен проводитися антивірусний контроль всіх дисків і файлів РС.

Обов'язковому антивірусному контролю підлягає будь-яка інформація (текстові файли будь-яких форматів, файли даних, виконувані файли), одержувана і передана по телекомунікаційних каналах, а також інформація на знімних носіях (CD-ROM і т.п.). Розархівація і контроль вхідної інформації необхідно проводити безпосередньо після її прийому на виділеному автономному комп'ютері або, за умови початкового завантаження ОС в оперативну пам'ять комп'ютера з завідомо «чистої» (не зараженої вірусами) і захищеною від запису системної дискети, - на будь-якому іншому комп'ютері. Можливе застосування іншого способу антивірусного контролю вхідної інформації, що забезпечує аналогічний рівень ефективності контролю. Контроль вихідної інформації необхідно проводити безпосередньо перед архівуванням і відправкою (записом на знімний носій). Файли, що поміщаються в електронний архів повинні в обов'язковому порядку

проходити антивірусний контроль. Періодичні перевірки електронних архівів мають проводитися не рідше одного разу на місяць.

При виникненні підозри на наявність комп'ютерного вірусу (нетипова робота програм, поява графічних і звукових ефектів, спотворень даних, пропажа файлів, часта поява повідомлень про системні помилки і т.п.) співробітник відділу самостійно повинен провести позачерговий антивірусний контроль своєї РС. При необхідності залучити фахівців відділу інформаційних технологій для визначення ними факту наявності або відсутності комп'ютерного вірусу.

У разі виявлення при проведенні антивірусної перевірки заражених комп'ютерними вірусами файлів співробітники відділу зобов'язані:

– призупинити роботу;

– негайно поставити до відома про факт виявлення заражених вірусом файлів співробітників відділу інформаційних технологій та співробітників відділу безпеки, власника заражених файлів, а також суміжні відділи, які використовують ці файли в роботі;

– провести лікування або знищення заражених файлів (при необхідності для виконання вимог даного пункту залучити фахівців відділу інформаційних технологій);

– у разі виявлення нового вірусу, що не піддається лікуванню застосовуваними антивірусними засобами, направити заражений вірусом файл на гнучкому магнітному диску у відділ інформаційних технологій для подальшої передачі його в організацію, з якою укладено договір на антивірусну підтримку;

– за фактом виявлення заражених вірусом файлів скласти службову записку до відділу безпеки, в якій необхідно вказати Можливий джерело (відправника, власника і т.д.) зараженого файлу, тип зараженого файлу, характер міститься у файлі інформації, тип вірусу і виконані антивірусні заходи.

2 Відповідальність

Відповідальність за організацію антивірусного контролю робочої станції покладається на користувача робочої станції.

Наказ про створення робочої групи щодо проведення категоріювання виділених приміщень та підготовки проєктних документів стосовно організаційного захисту інформації ОІД ТОВ «МонтажЕнерго» наведений у Додатку Г, а акт категоріювання вказаного об’єкту – у Додатку Ґ.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на реалізацію політики безпеки

Розробка політики безпеки супроводжується різними витратами, пов'язаними з оплатою праці розроблювачів, необхідністю реалізації проєктно-архітектурних рішень, придбанням, встановленням та налагодженням засобів та заходів захисту інформації.

Метою економічного розділу є визначення витрат на розробку політики безпеки, передбачуваних збитків за умови успішної атаки на активи підприємства, оцінка економічного ефекту й рентабельності.

3.2 Визначення трудомісткості розробки системи інформаційної безпеки

Трудомісткість створення системи визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації.

$$t = t_{тз} + t_в + t_а + t_{пр} + t_{опр} + t_д, \text{ год.}$$

Де $t_{тз}$ = 8 год. – тривалість складання технічного завдання на розробку системи;

$t_в$ = 10 год. – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

$t_а$ = 6 год. – тривалість розробки системи;

$t_{пр}$ = 6 год. – тривалість програмування за готовою системою;

$t_{опр}$ = 4 год. – тривалість опрацювання системи підтримки;

$t_д$ = 4 год. – тривалість підготовки технічної документації.

$$t = 8 \text{ год.} + 10 \text{ год.} + 6 \text{ год.} + 6 \text{ год.} + 4 \text{ год.} + 4 \text{ год.} = 38 \text{ год.}$$

3.3 Розрахунок витрат на створення системи інформаційної безпеки

Витрати на створення системи інформаційної безпеки Крп складаються з витрат на заробітну плату виконавця розробки Ззп і вартості витрат машинного часу, що необхідний для опрацювання алгоритму на ПК Змч:

$$Крп = Ззп + Змч,$$

де Крп – витрати на створення системи інформаційної безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення системи ІБ.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$Ззп = t * Зіб = 38 * 275 = 10450 \text{ грн.}$$

де t – загальна тривалість розробки системи підтримки, год.;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 275 грн/год.

Вартість машинного часу для розробки системи інформаційної безпеки на ПК визначається за формулою:

$$Змч = t * Смч, \text{ грн.},$$

де t – трудомісткість розробки системи ІБ на ПК, год.;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P * tнал * Се + \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{Fp} =$$

$$= 0,3 * 1 * 6 + (28000 * 0,5)/1920 + (25000 * 0,5)/1920 =$$

$$= 1,8 + 7,29 + 6,51 = 15,6;$$

де Р- встановлена потужність апаратури інформаційної безпеки, 0,3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин, на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 6 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 28000 грн.;

На – річна норма амортизації на ПК, 0.5 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,5 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 25000 грн.;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год.).

$$Змч = t * Смч = 38 * 15,6 = 592,8 \text{ грн.}$$

Визначена таким чином вартість створення системи ІБ Крп є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

$$Крп = Ззп + Змч = 10450 + 592,8 = 11042,8 \text{ грн.}$$

3.4 Розрахунок капітальних витрат

Капітальні (фіксовані) витрати на проєктування та впровадження проєктного варіанта системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн,$$

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 25000 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, 65000 грн.;

Крп – вартість розробки політики безпеки інформації, 11042,8 грн.;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів, 32000 грн.;

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу (навчання адміністратора), 15000 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки входять до заробітної плати адміністратора, 0 грн.

Відповідно до заданих даних розраховуємо капітальні витрати

$$К = Кпр + Кзпз + Крп + Каз + Кнавч. + Кн =$$

$$= 25000 + 65000 + 11042,8 + 32000 + 15000 = 148042,8 \text{ грн.}$$

3.5 Розрахунок експлуатаційних витрат

Поточні витрати включають:

– навчання персоналу в питаннях інформаційної безпеки;

– витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 15000 грн. – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 2000 + 1500 = 3500 \text{ грн. (в міс.)}$$

$$Сз = 3500 * 12 = 42000 \text{ грн. (рік),}$$

де Зк – додаткова заробітна плата керівника, 24000 грн. на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 18000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це,$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*8 комп'ютерів = 2,4 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 8 комп'ютерів = 15360 год. – річний фонд робочого часу системи інформаційної безпеки;

Це = 6 грн за 1 кВт/год. – тариф на електроенергію на 01.01.2024 року.

$$Се = 2,4 * 15360 * 6 = 221184 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 148042,8 * 0,02 = 2960,86 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Сз + Се + Стос =$$
$$= 15000 + 42000 + 221184 + 2960,86 = 281144,86 \text{ грн.}$$

3.6 Розрахунок оцінки величини збитку

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Місячний фонд робочого часу складає 176 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 3 год.

$$Пп = (Зс/Fр) * tп = (315000/176) * 3 = 5369,32 \text{ грн.},$$

де Зс – сумарна заробітна плата персоналу, 315000 грн.

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу тви = 3 год.:

$$Пви = (315000/176) * 3 = 5369,32 \text{ грн.}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год. і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = 275 * 4 = 1100 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч =$$

$$= 5369,32 + 1100 + 5000 = 11469,32 \text{ грн.},$$

де Пзч = 5000 грн. - вартість для витрат на заміну частин.

О = 10550000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = O/Fp * (tп + tв + tви) = 10550000/1920 * (3 + 4 + 3) = 54947,92 \text{ грн.}$$

Fp – це річний фонд часу роботи офісу, 1920 годин;

tп – 3 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 3 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на інформаційну систему при реалізації загрози складе:

$$U = Пп + Пв + V =$$

$$= 5369,32 + 11469,32 + 54947,92 = 71786,56 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum i \sum n * U = 8 * 4 * 71786,56 = 2297169,92 \text{ грн.},$$

де: i- число атакованих вузлів, 8 комп'ютерів;

n – середнє число атак на рік, 4 рази.

3.7 Визначення загального ефекту від впровадження системи захисту інформації

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням B – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R – C = 2297169,92 * 0.25 - 281144,86 = 293147,62 \text{ грн.}$$

3.8 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій To.

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

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = E/K = 293147,62 / 148042,8 = 1,98$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1/1,98 = 0,5 \text{ року} = 6 \text{ місяців}.$$

3.9 Висновок

У цьому розділі обґрунтована економічна доцільність впровадження політики безпеки для об'єкта ОІД ТОВ «МонтажЕнерго». Для обґрунтування доцільності були визначені наступні фактори:

– загальні витрати на впровадження політики безпеки на підприємстві;

– передбачувані збитки за умови успішної інформаційної атаки на підприємство.

За отриманими результатами можна зробити висновок, що при атаці загальна сума збитків буде складати 2297169,92 грн. При цьому поточні експлуатаційні витрати складають 281144,86 грн, а капітальні інвестиції - 148042,8 грн., що значно менше ніж можливі збитки.

Відповідно до розрахунків, виконаних в даному розділі, запропонована система захисту інформації є економічно вигідною.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено обстеження ТОВ «МонтажЕнерго». Були виявлені джерела загроз, загрози та вразливості інформації, яка циркулює в ТОВ «МонтажЕнерго». Після складання моделі загроз була розроблена політика безпеки, яка дозволяє суттєво підвищити рівень інформаційної безпеки на підприємстві.

У економічному розділі була розрахована економічна доцільність запропонованої політики безпеки.

Практична цінність кваліфікаційної роботи полягає в підвищенні рівня безпеки інформації, що циркулює в ТОВ «МонтажЕнерго», шляхом впровадження розробленої політики безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
2. Постанова «Про затвердження Порядку визначення розміру збитків від розкрадання, нестачі, знищення (псування) матеріальних цінностей» // (Електрон. ресурс) / Спосіб доступу: URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=116-96-%EF – Назва з екрана.
3. Закон України «Про інформацію».
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
5. НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".
6. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97.
7. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 2.5-005-99 від 28.04.99 №22 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
8. Кібербезпека України: аналіз сучасного стану / Трофименко О., Прокоп Ю., Логінова Н., Задерейко О.; [Електронний ресурс] – Режим доступу до ресурсу:http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y
9. Модель порушника. [Електронний ресурс]. – Режим доступу: https://studfiles.net/preview/4485292/page:5/. Назва з екрана.
10. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Розділ 1	34	
6	А4	Розділ 2	22	
7	А4	Розділ 3	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	2	
15	А4	Додаток Д	1	
16	А4	Додаток Е	2	

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Презентація_ Рябчинська.ppt
2. Кваліфікаційна робота_ Рябчинська.doc

ДОДАТОК В. План розташування ТОВ «МонтажЕнерго»

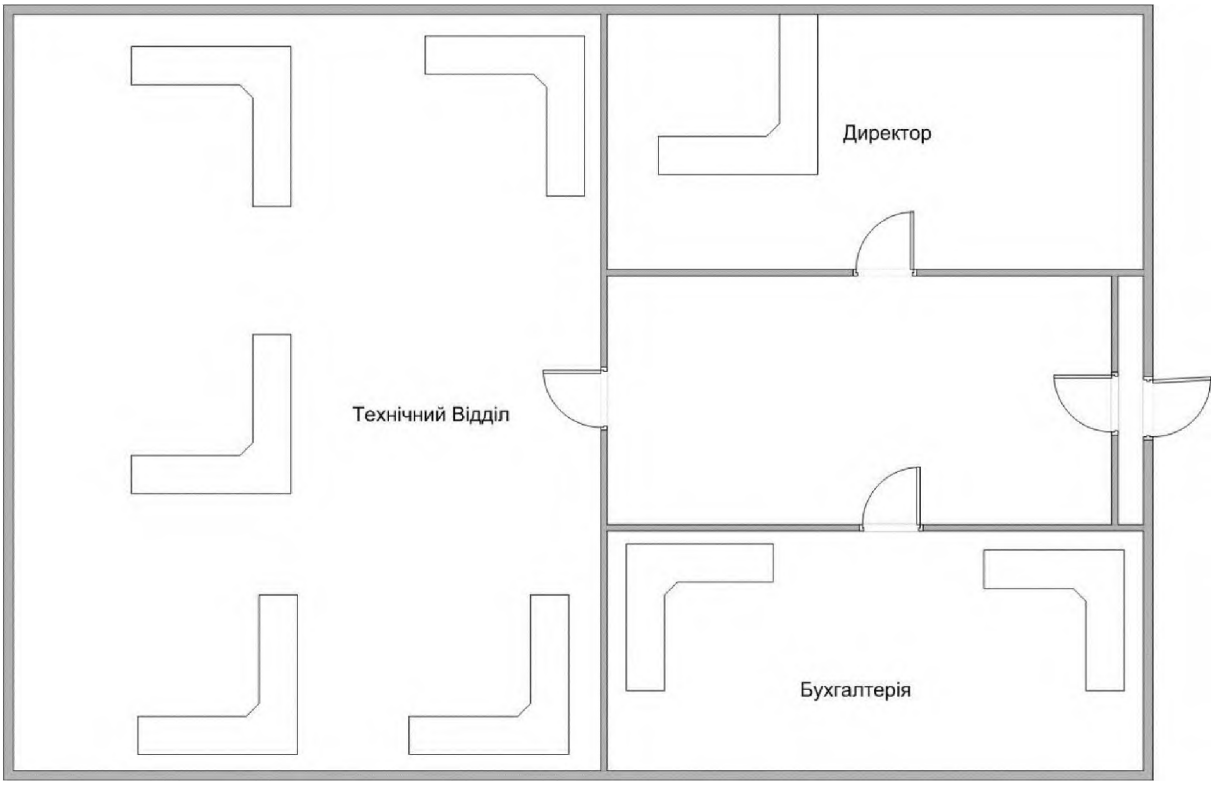

Рисунок В.1 – План розташування ТОВ «МонтажЕнерго»

ДОДАТОК Г. Наказ про проведення категоріювання

ТОВ «МонтажЕнерго»

НАКАЗ № 63

08.01.24 м. Кам’янське

Про створення робочої групи щодо проведення категоріювання виділених приміщень та підготовки проєктних документів стосовно організаційного захисту інформації ОІД ТОВ «МонтажЕнерго»

НАКАЗУЮ:

1 Створити робочу групу для проведення категоріювання виділених приміщень – ТОВ «МонтажЕнерго» та об’єктів електронної обчислювальної техніки, що знаходиться у цьому приміщенні, у складі:

Системний адміністратор ТОВ «МонтажЕнерго» – Іванов І.І. - голова робочої групи;

Члени робочої групи: заступник директора ТОВ «МонтажЕнерго» - Скарбицький П.С.

2 Робочій групі у термін до 22.01.24 включно підготувати пропозиції щодо наступних питань: перелік ІзОД, планування заходів з ОЗІ, наявність нормативно-методичної документації, , протокол про визначення вищого ступеня обмеження доступу до інформації (НД ТЗІ 1.1–005–07), модель загроз, модель порушника (ситуаційний, генеральний план).

3 Результати діяльності комісії представити у вигляді: актів, рекомендацій щодо створення, вдосконалення нормативно-методичної

документації.

4 Контроль за виконання поставлених завдань покласти на системного адміністратора ТОВ «МонтажЕнерго».

5 Відповідальність за діяльність робочої групи та виконання даного наказу залишаю за собою.

Директор

ТОВ «МонтажЕнерго»

_____

ДОДАТОК Ґ. Акт категоріювання

ЗАТВЕРДЖУЮ

Директор

ТОВ «МонтажЕнерго»

_____

«23» січня 2024 р.

АКТ № 1

_____

Категоріювання об’єкту інформаційної діяльності

ТОВ «МонтажЕнерго»

23.01.24 м. Кам’янське

Комісія в складі:

Системний адміністратор ТОВ «МонтажЕнерго» Іванов І.І. – голова робочої групи;

Члени робочої групи: заступник директора ТОВ «МонтажЕнерго» – Скарбицький П.С.

Призначена наказом № 1 від 08.01.2024 провела категоріювання приміщення ОІД ТОВ «МонтажЕнерго».

Комісія розглянула та проаналізувала:

Об’єктами категоріювання є об’єкти інформаційної діяльності, в тому числі об’єкти ІКС.

Комісія постановила:

1 Підстава для категоріювання: НАКАЗ № 63 «Про створення робочої групи щодо проведення категоріювання виділених приміщень та підготовки проєктних документів стосовно технічного захисту інформації ОІД ТОВ «МонтажЕнерго».

2 Вид категоріювання – первинне.

3 На ОІД здійснюється обробка інформації технічними засобами та озвучування інформації.

4 Ступінь обмеження доступу до інформації, що обробляється технічними засобами та озвучується на об'єкті – конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації».

5 Встановлена категорія - четверта.

Комісія в складі:

Голова: Системний адміністратор ТОВ «МонтажЕнерго»

Іванов І.І._____

Члени: програміст, заступник директора ТОВ «МонтажЕнерго»

Скарбицький П.С. _____

ДОДАТОК Д. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-20-1 Рябчинської В.К. на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «МонтажЕнерго»

Пояснювальна записка містить 83 сторінки, 2 рисунки, 8 таблиць, 7 додатків, 10 джерел.

Метою даної кваліфікаційної роботи є підвищення рівня захисту інформації з обмеженим доступом, яка циркулює в ТОВ «МонтажЕнерго».

У ході виконання роботи було виявлено загрози безпеки ТОВ «МонтажЕнерго» та вжиті заходи щодо усунення потенційних загроз. Було виконано обстеження об'єкту інформаційної діяльності, проаналізовано інформаційні потоки, проведено аналіз загроз та вразливостей системи, побудована модель порушника. Також обґрунтовано вибір стандартного функціонально профіля захищеності та розроблено інструкції політики безпеки.

В економічному розділі був виконаний розрахунок збитку від реалізації загрози та визначені витрати на створення засобів забезпечення інформаційної безпеки підприємства.

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків завдяки впровадженню політики забезпечення інформаційної безпеки.

В якості недоліків кваліфікаційної роботи слід визначити наступне: незначні невідповідності вимогам при оформленні.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її авторка Рябчинська В.К. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
д.т.н., проф. **Корченко А.В.**