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

студента *Глухих Ростислава Олександровича*

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 «Аквамарин»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
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

студенту ***Глухих Р.О.*** **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 «Аквамарин»***

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

Розділ	Зміст	Термін виконання
1	Стан питання, аналіз нормативно-правової бази, постановка задачі.	26.05.2024
2	Розробка політики безпеки інформації, визначення профілю захищеності, аналіз загроз.	19.06.2024
3	Розрахунок річних витрат на розробку політики безпеки, оцінка величини збитку. Розрахунок ефективності.	26.06.2024

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Глухих Р.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 94 сторінки, 5 рисунків, 15 таблиць, 4 додатки, 15 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи.

Мета кваліфікаційної роботи: підвищення рівня інформаційної безпеки ІКС ТОВ «Аквамарин».

В ході виконання кваліфікаційної роботи було розглянуто та проаналізовано: найбільш актуальні загрози інформаційній безпеці для малих комерційних підприємств; розглянута узагальнена методика управління ризиками та система управління інцидентами інформаційної безпеки; розглянуті основні принципи, на яких повинна базуватися політика безпеки інформації на підприємстві; проведено аналіз нормативно-правової бази у сфері захисту інформації; виконана постановка задачі кваліфікаційної роботи.

В другому розділі було проведено обстеження об'єкта інформаційної діяльності; визначено і виконано категоріювання інформації, що циркулює в інформаційній системі; розроблено аналіз загроз та порушника; розроблено політику безпеки інформації для інформаційної системи.

В економічній частині розраховано витрати на розробку політики безпеки ТОВ «Аквамарин».

Практична цінність кваліфікаційної роботи полягає у підвищенні рівня інформаційної безпеки та зниженні ризиків завдяки впровадженню запропонованої політики безпеки інформації інформаційно-комунікаційної системи підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ.

ABSTRACT

The explanatory note consists of 94 pages, 5 images, 15 tables, 4 appendices, 15 sources.

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

The purpose of the qualification work: to increase the level of information security of the ICS of "Aquamarine" LLC.

In the course of the qualification work, the following were considered and analyzed: the most relevant threats to information security for small commercial enterprises; the generalized risk management technique and information security incident management system are considered; the main principles on which the information security policy at the enterprise should be based are considered; an analysis of the legal framework in the field of information protection was carried out; the statement of the task of the qualification work has been completed.

In the second section, an examination of the object of information activity was carried out; the information circulating in the information system has been categorized and performed; an analysis of threats and the violator was developed; an information security policy for the information system was developed.

In the economic part, the costs for the development of the security policy of "Aquamarine" LLC are calculated.

The practical value of the qualification work is to increase the level of information security and reduce the risks of information security due to the implementation of information security policy.

INFORMATION SAFETY, MODEL OF THREATS, USER VIOLATOR MODEL, INFORMATION SECURITY POLICY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

ІТ – інформаційні технології;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПБ – політика безпеки.

ЗМІСТ

ВСТУП

У сучасному світі все більше виробництв і послуг спираються на інформаційні технології: виробництво і постачання енергії, очищення і постачання питної води, керування транспортом, освітлення міст, доступ людей до інформації, охорона здоров'я, оплата товарів і послуг і навіть електронне урядування – все це реалії нашого життя. Ми залежимо від безперервності та коректності функціювання комп'ютерних систем об'єктів критичної інфраструктури. Атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства. На сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів. Щодня кожен з нас стикається із необхідністю користування інформаційними технологіями: від соціальних мереж, розміщення інформації про свої персональні дані в інтернеті до користування банкоматами, банківськими рахунками тощо. У зв'язку із цим виникає питання, чи врегульовано дану проблему вітчизняним законодавством і як себе захистити від кіберзлочинців.

Аналіз українського законодавства дав зрозуміти, що, на жаль, в Україні на сьогодні, навіть не визначено таких ключових понять: кіберзлочин, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист.

Водночас спостерігається вільне використання значної кількості термінів (та їх синонімів), що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», причому жоден з цих термінів не має свого визначення ані в цьому, ані в інших нормативних документах. В Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а ті елементи, що можуть до нього відноситись прописані як складова частина поняття «технологічний тероризм». У «Стратегії національної безпеки України» комп'ютерні загрози не згадуються, а «кібербезпека» – лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з

вимогами ратифікованої Верховною Радою України «Конвенції про кіберзлочинність». Однак оприлюднена редакція «Стратегії національної безпеки» 2011 року вже використовує термін «кібербезпека».

В «Доктрині інформаційної безпеки України» також згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», знову ж таки – без жодних пояснень чи посилання на такі пояснення. Крім того, в Доктрині згадуються і «кібератаки» без визначення терміну. Отже, можна констатувати, що в більшості своїй українське нормативно-правове поле в сфері інформаційної (кібернетичної) безпеки оперує термінами визначень яких фактично немає.

Варто відмітити, що дане питання повільно, але все ж таки вирішується. Згідно із законом, «кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі[1]; кібернетичний простір (кіберпростір) – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На сьогодні актуальність проблеми кібербезпеки дуже широко розповсюджена на комерційних підприємствах. В даній кваліфікаційній роботі, буде розглянуто мале комерційне підприємство. Для того, щоб перейти до більш детального аналізу підприємства, розглянемо основні загрози, ризики, інциденти та політику безпеки в інформаційній безпеці.

На підприємстві існують основні загрози інформаційній безпеці.

Дестабілізуючі фактори — явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції ворожих держав, в яких для формування інформаційних загроз створюються і функціонують спеціальні органи і служби.

Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів відносять:

– правовий вакуум у більшості питань забезпечення інформаційної безпеки;

– навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;

– політичні конфлікти;

– зловмисні дії злочинних елементів або груп;

– відмови, збої, технічні помилки інформаційних систем (засобів);

– природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори — це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т.ін.).

Класифікація загроз інформаційній безпеці

Загрози інформаційній безпеці — сукупність умов і факторів, що створюють небезпеку життєвоважливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого і не правомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т.ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні (рисунок. 1.1).

Рисунок. 1.1 - Класифікація загроз інформаційній безпеці

Під політичними факторами загроз інформаційній безпеці розуміють:

– зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

– інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

– становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

– знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

– порушення інформаційних зв'язків унаслідок утворення на території колишнього СРСР нових держав;

– прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

– низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є :

– недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері. Ієрархічна класифікація загроз інформаційній безпеці. Глобальні фактори загроз інформаційній безпеці:

– недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження інформації та нових інформаційних технологій;

– діяльність іноземних розвідувальних та спеціальних служб;

– діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави;

– злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці:

– використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації;

– невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами;

– відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій;

– недопустимо високий рівень технологічної залежності держави від зарубіжних держав у зв'язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій;

– розвиток зарубіжних технічних засобів розвідки, та промислового шпигунства, що дозволяє одержати несанкціонований доступ до конфіденційної інформації, у тому числі такої що складає державну таємницю;

– зростання злочинності в інформаційній сфері;

– використання старих методів та засобів захисту національних інформаційних мереж, широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку;

– відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

Локальні фактори загроз інформаційній безпеці:

– перехоплення електронних випромінювань;
– застосування підслуховуючих пристроїв або закладок;
– дистанційне фотографування;
– розкрадання носіїв інформації та промислових відходів;
– копіювання носіїв інформації з подоланням заходів захисту;
– незаконне приєднання до апаратури та ліній зв'язку;
– упровадження та використання комп'ютерних вірусів і т.ін.

Розглянемо основні ризики на підприємстві.

Захист інформаційних ресурсів повинен бути продуманий ефективно, оскільки він в граничному ступені призначений і для збереження фінансових ресурсів підприємства.

Оцінка ризиків – частина напрямки інформаційної безпеки – управління ризиками.

Принцип визначення необхідного рівня захисту: «Сума витрат на забезпечення захисту не повинна «перевершувати суми збитку від атаки, яку даний захист повинен запобігти».

По суті, ризик як такої і складається з поняття ймовірності, тобто чим більша ймовірність 1,2,3, - тим більше ризик, і навпаки.

Оцінку втрати або знищення апаратно-технічної складової виробляти досить просто, бо відома ринкова вартість, значно важче відповісти на питання який буде збиток від:

– порушення конфіденційності, цілісності, доступності;
– відновлення (заміна) при її втраті (знищенні).

Розглянемо методику управління ризиками:

– визначення політики управління ризиками (на загальноприйнятих принципах інформаційної безпеки) щоб уникнути суб'єктивного підходу;
– визначення персоналу, який буде займатися УР (тут: оплата праці, навчання кадрів, придбання платних методик оцінки ризиків, автоматизованого інструментарію) ;

– ідентифікація та вимірювання ризиків (загрози, IP і інформативний і їхню соціальну значимість; уразливості активів, які можуть вплинути на частоту появи або розмір можливого збитку - за окремими методиками).

– встановлення критеріїв прийнятності ризиків (наприклад, ймовірність втрати 10 тис. у.о. більше 3%, або ін.) ;

– уникнення і зменшення ризиків: необхідно визначити уразливості, які стають неприйнятними при прийнятих умовах і визначити заходи для їх усунення (відповідність між ціною коштів та їх ефективністю), звіт керівнику;

– моніторинг робіт з управління ризиками. Для забезпечення адекватності вжитих заходів відповідним ризикам, необхідно вживати превентивних заходів: переоцінку ризиків при зміні зовнішніх або внутрішніх загроз і ін.

Розглянемо основну систему управління інцидентами інформаційної безпеки.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки(згідно з ГСТУ СУІБ 1.0/ISO/IEC 27001:2010)[2]. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам. Для найбільш ефективної реалізації системи управління інцидентами інформаційної безпеки необхідно спиратись на вимоги міжнародних і галузевих стандартів.

Управління інцидентами, це важливий процес, який забезпечує організації можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі управління інцидентами:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливіших напрямах;
- надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Управління інцидентами і проблемами є комплексним рішенням, що оптимізує управління всіма аспектами обслуговування і підтримки, необхідними для підприємства.

Використовуючи кращі, перевірені часом, напрацювання і вирівнювання IT-процесів для обробки збоїв будь-яких видів, рішення з управління інцидентами дозволяють використовувати ресурси залежно від пріоритетів ділової діяльності, управляти рівнями обслуговування, а також краще контролювати витрати IT-служб.

Рішення з управління інцидентами прискорює процес вирішення інцидентів на всіх етапах: від первинного виявлення і діагностики проблем та основних причин до остаточного їх усунення.

Для реалізації системи управління інцидентами інформаційної безпеки необхідно провести наступні роботи:

- виділити ресурси для розробки та впровадження системи управління інцидентами;
- визначити область функціонування системи управління інцидентами;
- розробити комплекс процесів системи управління;
- навчити персонал;
- впровадити процеси управління інцидентами та інтегрувати їх зі вже функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності;

– розробити архітектуру і комплекс технічних засобів з автоматизації процесів управління інцидентами і моніторингу подій інформаційної безпеки;

– впровадити комплекс програмно-технічних засобів автоматизації управління інцидентами.

В результаті проведених робіт буде впроваджена система управління інцидентами інформаційної безпеки, яка буде вирішувати наступні задачі:

– оперативний моніторинг стану інформаційної безпеки в рамках обраної галузі діяльності системи;

– виявлення, облік, реагування, розслідування та аналіз інцидентів інформаційної безпеки.

Розглянемо політику безпеки інформації на підприємстві. Під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз(згідно з НД ТЗІ 1.1 003.99). . Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. Як складові частини загальної політики безпеки мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації ,взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів політика безпеки стосується, а яких – ні).

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.

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 автоматизованій системі (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;

– реалізація заходів захисту інформації є рентабельною;

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

– забезпечується персоніфікація положень політики безпеки ,звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування автоматизованої системи;

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

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

– враховані вимоги всіх документів, які регламентують порядок захисту інформації в автоматизованій системі та забезпечується їхнє суворе дотримання.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Під поняттям нормативно-правового бази слід розуміти сукупність правових норм, що визначають порядок створення, правовий статус і функціонування захищених інформаційно – комунікаційних систем, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Тобто нормативно-правове забезпечення показує та визначає:

– порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі;

– регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації;

– статус інформаційної системи з точки зору інформаційної безпеки;

– права, обов'язки й відповідальність персоналу роботи яких пов’язані з інформаційною безпекою; правові положення окремих видів процесу керування та управління доступом в захищених ІКС; порядок створення й використання захищених інформаційно – комунікаційна система.

Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів слід керуватися низкою нормативно-правових документів та актів.

Базовими нормативними документами при організації та побудови комплексної системи захисту інформації в інформаційно – комунікаційній системі є:

– Закон України «Про інформацію»;

– Закон України «Про захист інформації в автоматизованих системах»;

– НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

– НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

– НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53);

– НД ТЗІ 2.5-005-99: 2012 60 автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

– НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).;

– НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. № 22)

1.3 Постановка задачі

В даній кваліфікаційній роботі повинна бути розроблена політика безпеки в інформаційно-комунікаційній системі. Дана кваліфікаційна робота буде розроблятися про мале комерційне підприємство на базі аналізу Розділу 1.

В розробці політики безпеки потрібно вказати загальні відомості про підприємство, обстежити ОІД цього підприємства, зробити аналіз ризиків з моделлю загроз та порушника, обґрунтувати необхідність створення КСЗІ, розробити політику безпеки та проаналізувати ризики після впровадження політики безпеки.

Розробка політики безпеки інформаційно-комунікаційної системи є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної інформаційно – комунікаційної системи політика безпеки інформації може бути

індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама інформаційно – комунікаційна система може реалізовувати декілька різноманітних технологій обробки інформації, тоді і політика безпеки інформації в такій інформаційно – комунікаційній системі буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Важливо розуміти, що перед впровадженням будь-яких технічних або організаційних заходів щодо захисту інформації, необхідно розробити політики безпеки, адекватні цілям і завданням бізнесу підприємства. Система ІБ буде ефективною, якщо вимоги, засоби, що реалізуються для підприємства гармонійно доповнюють один одного в досягненні спільних цілей.

1.4 Висновки до першого розділу

У даному розділі були розглянуті питання актуальності кібербезпеки в Україні:

– проаналізовані найбільш актуальні загрози інформаційній безпеці для малих комерційних підприємств;

– розглянута узагальнена методика управління ризиками та система управління інцидентами інформаційної безпеки;

– розглянуті основні принципи на яких повинна базуватися політика безпеки інформації на підприємстві;

– проведений аналіз нормативно-правової бази у сфері захисту інформації;

– виконана постановка задачі дипломного проекту;

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

В кваліфікаційній роботі розглянуто товариство з обмеженою відповідальністю «Аквамарин», яке займається:

– ремонт, обслуговування комп'ютерів і оргтехніки;
– заправка та відновлення картриджів для принтерів;
– продаж комп'ютерів і оргтехніки;

Форма власності: приватна.

Адреса: вул. Гагаріна 13/15 оф.724

Штат співробітників підприємства складається з 5 чоловік:

– Директор – 1;
– Бухгалтер – 1;
– Спеціаліст з обслуговування комп’ютерної техніки – 2 ;
– Прибиральниця – 1.

Обов’язки директора:

– забезпечує прийом обладнання, комплектуючих та матеріалів за кількістю і якістю;
– веде документообіг на фірмі;
– забезпечує виконання зобов'язань за договорами.

Обов’язки бухгалтера:

– виконує роботу з ведення бухгалтерського обліку майна, зобов'язань і господарських операцій (облік основних засобів, товарно-матеріальних цінностей, витрат на виробництво, реалізації продукції, результатів господарсько-фінансової діяльності; розрахунки з постачальниками і замовниками, за надані послуги і т.п.);
– виконує роботи з формування, ведення та зберігання бази даних бухгалтерської інформації, вносить зміни до довідкової та нормативної інформації, яка використовується при обробці даних.

Обов’язки спеціаліста з обслуговування комп’ютерної техніки:

– обслуговує, ремонтує та модернізує комп'ютери та оргтехніку;

– займається заправкою та відновленням картриджів для принтерів.

Співробітники компанії, окрім прибиральниця, працюють по будням з 09:00 до 18:00. Прибиральниця працює по вівторках з 08:00 до 09:00.

Збереження та захист інформації компанії «Аквамарин» повинні забезпечуватись згідно з Цивільним, Господарським кодексами та таких законів України: «Про захист персональних даних», «Про інформацію», «Про захист від недобросовісної конкуренції».

2.2 Обстеження об'єкту інформаційної діяльності

Об'єкт інформаційної діяльності – середовище, інженерно-технічна споруда, приміщення з визначеною контрольованою зоною, де здійснюється адміністративна, фінансово – економічна, виробнича, науково – технологічна та інша діяльність, пов'язана з інформацією, що підлягає захисту.

Таблиця 2.1 – Системи комунікацій підприємства

Системи комунікацій	Підключення
Електропостачання	підключено до трансформаторної підстанції. Виходити за межі контрольованої зони. Розетки і вимикачі - 220В.
Система каналізації	підключена до міської системи, яка виходить за межі контрольованої зони.
Система водопостачання	підключена до міськводоканалу, яка виходить за межі контрольованої зони.
Система опалення	підключена до міської системи опалення. Виходить за межі контрольованої зони
Вентиляція	здійснюється за допомогою кондиціонерів, які виходять за межі контрольованої зони.
Телефонна лінія	підключена до АТС «Укртелеком» і виходити за межі контрольованої зони

Продовження таблиці 2.1

Системи комунікацій	Підключення
Спосіб підключення до мережі Internet	кабельний інтернет
Заземлення	всі прилади, комп'ютери заземлені на загальний контур заземлення, який є замкнутим і виходить за межі КЗ

Розглянемо характеристику будівлі.

Офіс даної компанії знаходиться в будівлі, розташованій в житловій зоні. Він знаходиться на сьомому поверсі семиповерхової будівлі, облаштованого під офіси. Загальна площа 200 кв.м. Товщина несучих стін - 18 см. Товщина інших стін - 38 см. Висота всіх стін - 280 см. Матеріал - залізобетонні панелі. Профіль вікон - металопластик, товщина вікон - 3 мм. Вхідні двері виготовлені із заліза з дерев'яною обшивкою. Територія, навколо будівлі - відкрита, не обмежена забором. Перебування транспорту на цій території не обмежено та не контролюється. Територію навколо будівлі впорядковано, вона має асфальтове покриття.

Сусідні будівлі:

– Північ – Житлова будівля. У будівлі гуртожиток №2;

– Південь – Житловий багатоповерховий будинок;

– Захід – Адміністративна будівля. У будівлі знаходиться Національна металургійна академія України;

– Схід – Адміністративна будівля. У будівля знаходиться; відділення поштового зв’язку №3.

Розглянемо ситуаційний та генеральний план.

На ситуаційному плані (рисунок.2.1) показано місце розташування ОІД та розташовані навколо нього об’єкти. В таблиці 2.2 вказані умовні позначення на ситуаційному плані.

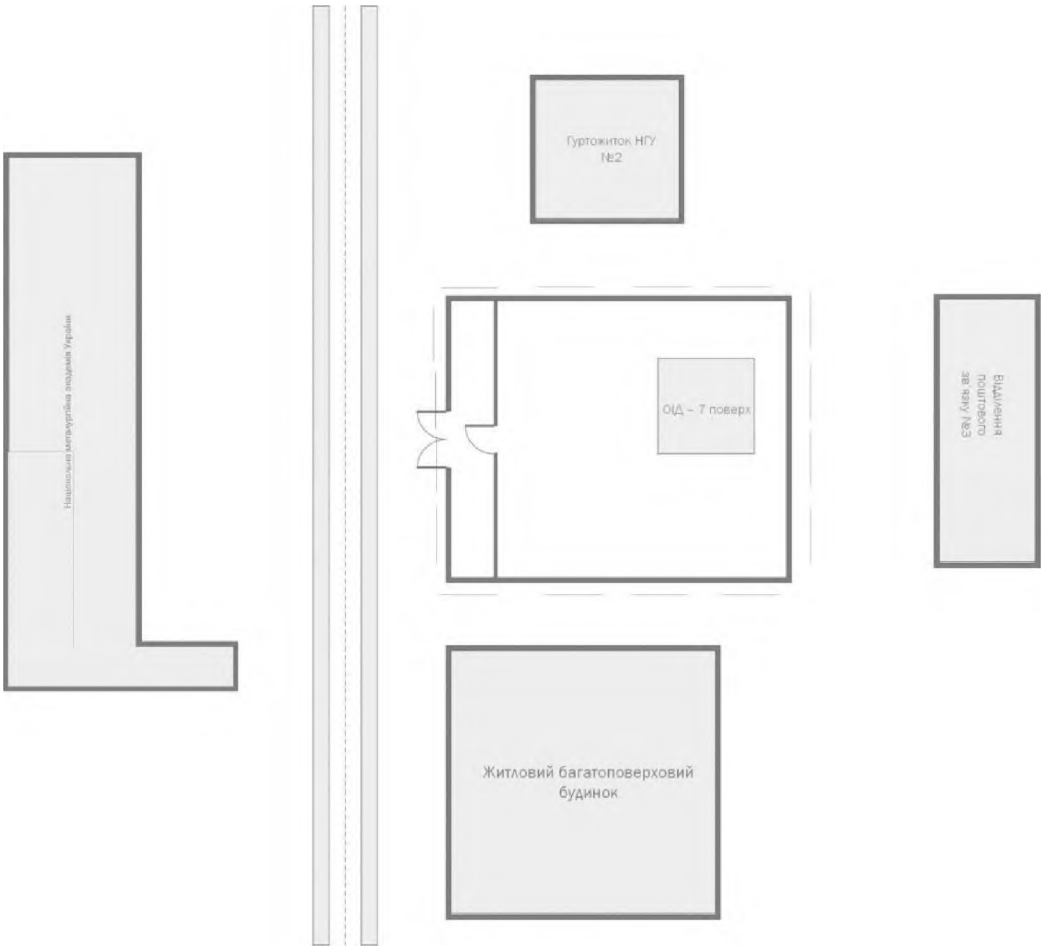
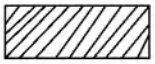


Рисунок 2.1 – Ситуаційний план ТОВ «Аквамарин»

Таблиця 2.2 – Умовні позначення

Позначка на плані	Значення
— · —	Межі споруди, в якій знаходиться ОІД
- · - · -	Межі ОІД
.....	Асфальтована дорога
	Каналізаційні труби

На ситуаційному плані (рисунок 2.2) показано місце розташування ОІД. У таблиці 2.3 показано умовні позначення генерального плану ТОВ «Аквамарин».

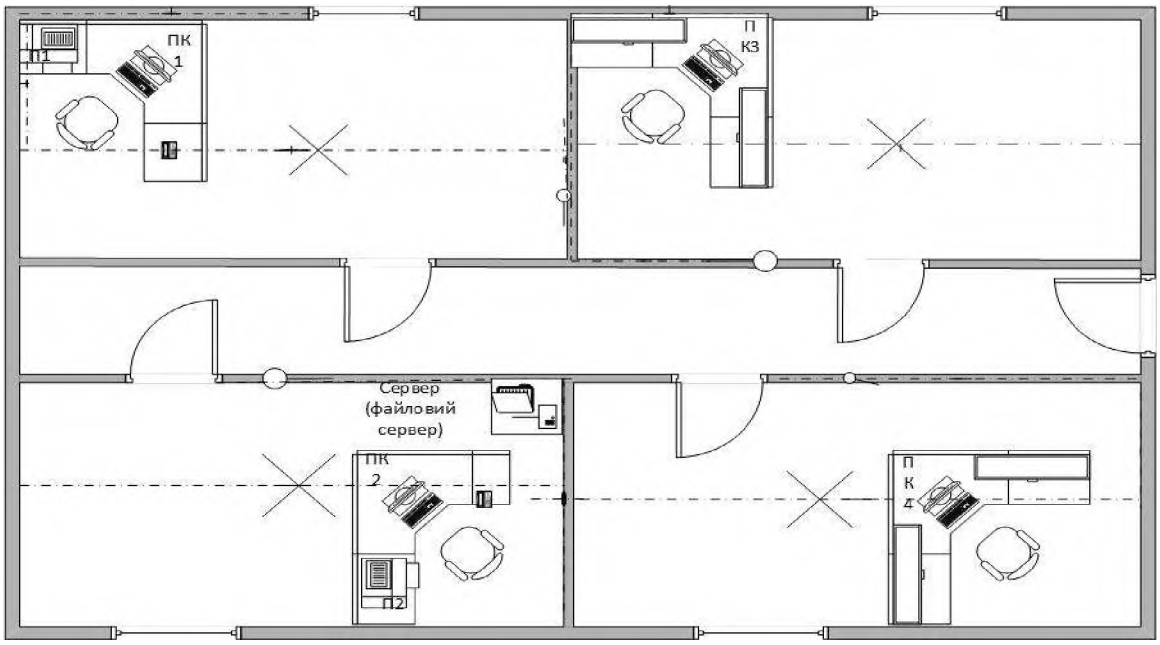
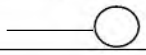


Рисунок 2.2 – Генеральний план ТОВ «Аквамарин»

Таблиця 2.3 Умовні позначення

Позначка на плані	Значення
— · —	Лінія системи електропостачання
	Лампа галогенна
	Вимикач

На рисунку 2.3 зображена схема мережі інформаційно–комунікаційної системи ТОВ «Аквамарин».

Схема мережі інформаційно-комунікаційної мережі містить ADSL modem (Internet), файловий сервер, 2 принтери (П1 та П2), switch та чотири комп’ютери (ПК1 – ПК4).

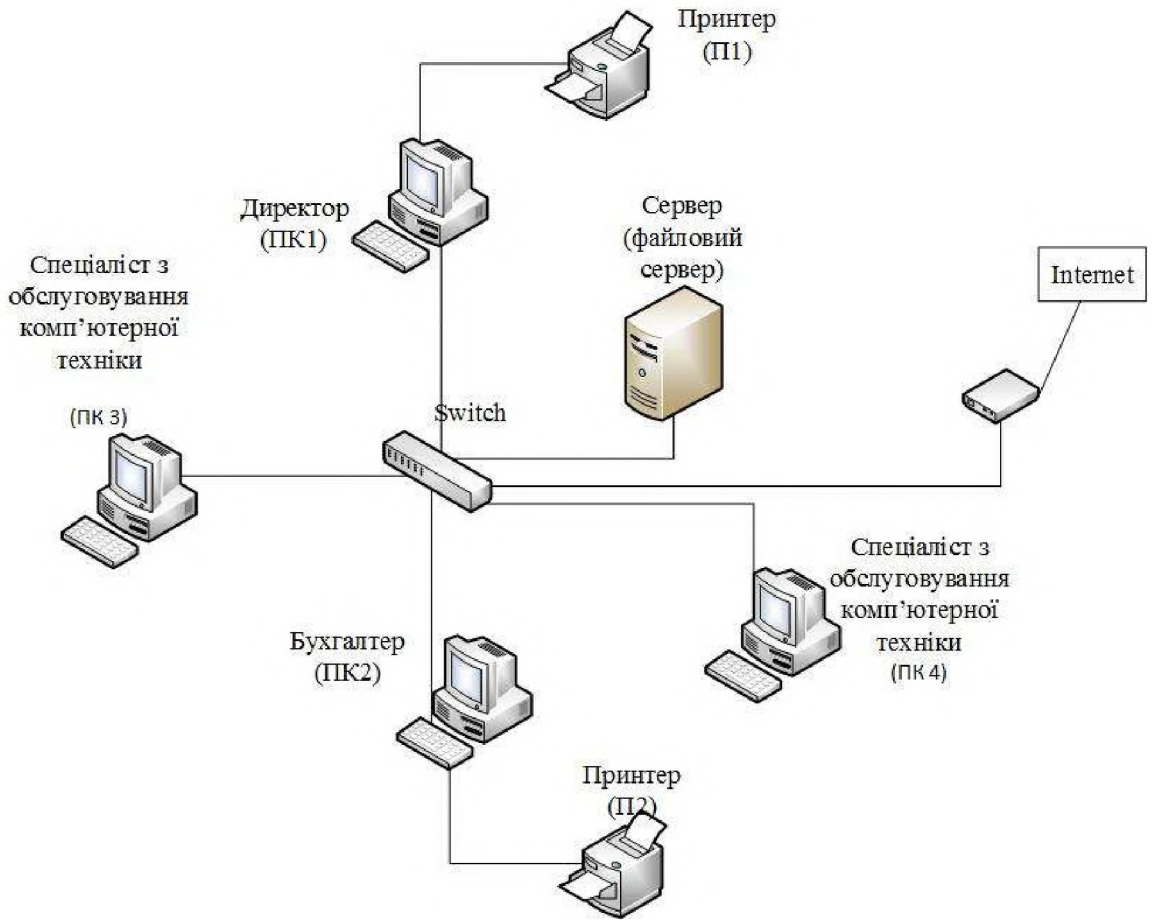


Рисунок 2.3 – Схема мережі ТОВ «Аквамарин»

У таблиці 2.4 показано інформацію, яка циркулює у ТОВ «Аквамарин»

Таблиця 2.4 – Інформація, яка циркулює у ТОВ «Аквамарин»

Інформація	Спосіб фіксації	Направлення руху	Стабільність	Приналежності до сфер діяльності	Час виникнення
Персональні дані співробітників	Усна/ документована/ цифрова	вхідна	Умовно-постійна	Оперативно-виробнича	поточна
Зміст та перелік договорів	Документована /цифрова	вхідна/ вихідна	Умовно - змінна	Оперативно-виробнича	минула/ поточна
Дані про рівень заробітної плати співробітників	Документована /цифрова	Вхідна/ вихідна	Змінна 1	фінансова	поточна

Продовження таблиці 2.4

1	2	3	4	5	6
Вартість і ціни обслуговування клієнтів	Документована/ цифрова	вхідна	змінна	фінансова	Поточна
Відомості про сплачення податків	Документована/ цифрова	вихідна	змінна	Планово–економічна	минула

У таблиці 2.5 представлений перелік апаратного, а в таблиці 2.6 - програмного забезпечення мережі ТОВ «Аквамарин».

Таблиця 2.5 – Апаратне забезпечення

№ п/п	Найменування	Модель
1	Сервер (файловий сервер)	SynologyDS216J/частота ЦП Два ядра 1.0 GHz/ кількість жорстких дисків 2(3.5 «SATA HDD;2.5» SATAHDD (with optional 2.5 «DiskHolder»)/ максимальна внутрішня ємність 20 TB (10 TB drive x 2)/зовнішні диски EXT4,EXT3,FAT/внутрішні диски EXT4/частота50/60 Hz, одна фаза
2	Принтер (П 1)	Canon PIXMA Ink Efficiency E414
	Принтер (П 2)	Canon PIXMA Ink Efficiency E414
3	Монітори (4шт.)	Philips V-line 193V5LSB2/62
4	Мишки (4 шт.)	Rival 95 Black (62347)
5	Модем	DSL LINKSYS X3500
6	Клавіатури(4шт)	Logitech K120 for Business
7	Системні блоки(4шт)	Lenovo Ideacentre 300-20ISH (90DA00HXRS)/Оперативна пам’ять (RAM) 8 ГБ/

Таблиця 2.6 – Програмне забезпечення

№ п/п	Тип ПЗ	Найменування	Обладнання
1	Операційна система	Windows 10	ПК1 – ПК4
		DiskStation Manager (DSM)	Сервер
2	Прикладне ПЗ	Microsoft Office 2013	ПК1-ПК4
3		Mozilla Firefox	
4		Windows Defender	
5		Nero 7	
6		Dilovod	ПК 1 – ПК 2
7	Спеціальне ПЗ	Adobe Reader	ПК 1 – ПК 4
8		Архиватор WinRar	
9		Skype	

У таблиці 2.7 подано перелік інформації, яка циркулює в ТОВ «Аквамарин».

Таблиця 2.7 – Перелік інформації

№ п/п	Інформація	Доступ до інформації	Вимоги до захисту.
1	Персональні дані співробітників	З обмеженим доступом	КЦД
2	Зміст та переліки договорів	відкрита	ЦД
3	Данні про рівень заробітної плати співробітників	З обмеженим доступом	КЦД
4	Вартість і ціни обслуговування клієнтів	відкрита	ЦД
5	Відомості про сплачення податків і зборів	відкрита	ЦД

Інформація, що циркулює в інформаційній системі в електронному вигляді та підлягає захисту щонайменше по одному показнику з основних властивостей інформації: конфіденційності, цілісності або доступності.

Наступна таблиця 2.8 – «Аналіз інформації, за критичністю основних властивостей» - детально демонструє яка властивість конкретної інформації потребує захисту.

Критерії оцінки:

За конфіденційністю:

– К4 – критична інформація, розголошування призведе до краху підприємства;

– К3 – важлива інформація, розголошування приведе до матеріальних збитків;

– К2 – значима інформація, може принести моральну шкоду;

– К1 – незначна інформація, яка не впливає на роботу.

За цілісністю:

– Ц4 – критична інформація, несанкціонована зміна якої приведе до неправильної роботи підприємства, наслідки такої модифікації незворотні;

– Ц3 – важлива інформація, несанкціонована зміна якої приведе до неправильної роботи підприємства через деякий час, наслідки зворотні;

– Ц2 – значна інформація, несанкціонована модифікація виявиться через деякий час, але не приведе до збою в системі, наслідки модифікації зворотні;

– Ц1 – незначна інформація, несанкціонована модифікація якої не позначиться на роботі системи.

– За доступністю:

– Д4 – критична інформація, робота підприємства буде зупинена;

– Д3 – важлива інформація, робота без неї можлива деякий час, але невдовзі вона знадобиться;

– Д2 – корисна інформація, без якої можна працювати, але її використання економить час;

– Д1 – неістотна інформація, яка не впливає на роботу.

Таблиця 2.8 – Аналіз інформації

Інформація	Важливість:		
	К	Ц	Д
Персональні дані співробітників	2	2	2
Зміст та перелік договорів	1	3	1
Дані про рівень заробітної плати співробітників	2	2	2
Вартість та ціни обслуговування	1	3	1
Відомості про сплачення податків та зборів	1	3	1

Розглянемо інформаційні потоки ТОВ «Аквамарин».

Інформаційні потоки - це фізичне переміщення інформації від одного співробітника підприємства до іншого або від одного підрозділу до іншого.

Система інформаційних потоків - це сукупність фізичних переміщень інформації, яка дає можливість здійснити який-небудь процес, реалізувати яке-небудь рішення.

Найбільш загальна система інформаційних потоків – це сума потоків інформації, яка дозволяє підприємству вести фінансово-господарську діяльність.

Інформаційні потоки забезпечують нормальну роботу підприємства. Ціль роботи з інформаційними потоками – оптимізувати роботу підприємства.

На рисунок 2.4 зображено інформаційні потоки ТОВ «Аквамарин»

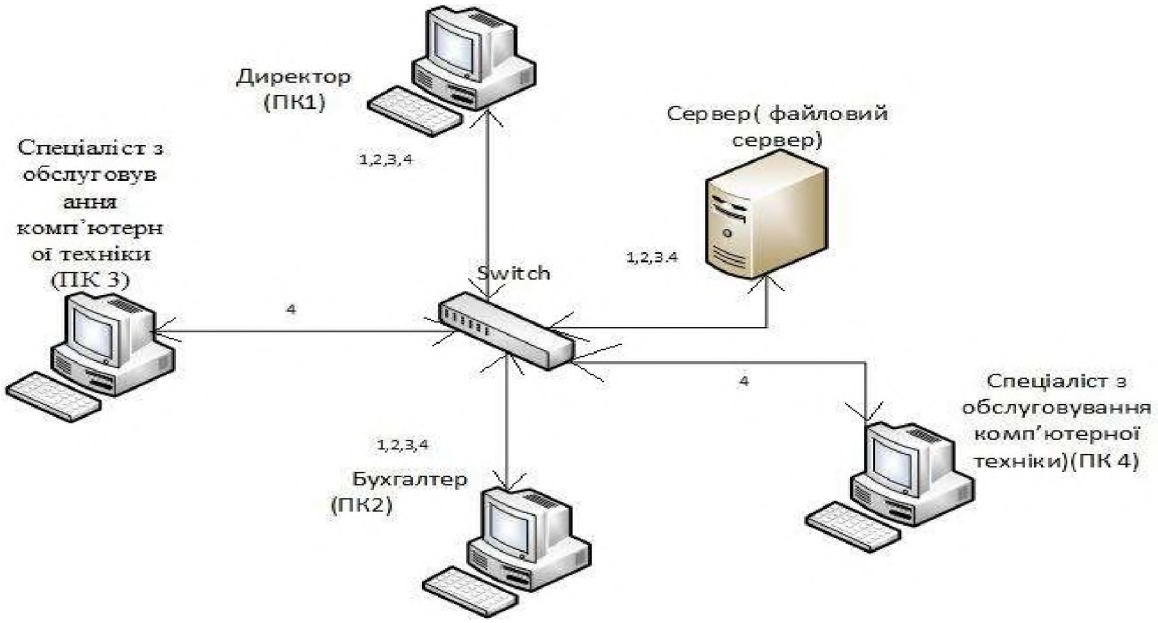


Рисунок 2.4 – Інформаційні потоки ТОВ «Аквамарин»

В таблиці 2.9 показано, яка інформація циркулює між співробітниками ТОВ «Аквамарин».

Таблиця 2.9 – Інформація, що циркулює між співробітниками

№ інформаційного потоку	Інформація, яка циркулює
1	Обробка інформації про персональні дані співробітників
2	Обробка бухгалтерської інформації
3	Обробка інформації, пов'язаної з договорами (порядок укладання, змісту)
4	Обробка інформації, пов'язаної з вартістю послуг, що надає підприємство

2.3 Аналіз ризиків

Загрози складають основу для оцінки ризиків. Для кожної визначаються п'ять ключових показників. Перш за все, це ціна втрати (кількісне вираження наслідків реалізації загроз) і величина уразливості (оцінка того, в якій мірі

вразливість знижує захищеність ресурсу). Після цього групи намагаються показати працюючі засоби контролю, здатні знизити ймовірність реалізації загрози. Потім проводиться перерахунок показника ймовірностей і з урахуванням впливу існуючих засобів контролю. На основі отриманих даних для кожної пари розраховується рівень ризику, відповідний конкретним загрозам.

Розглянемо аналіз загроз на підприємстві.

Класифікація загроз інформаційній безпеці. Можна стверджувати, що загрозами безпеці інформації є:

– розкрадання (копіювання) інформації;

– знищення інформації;

– модифікація (спотворення) інформації;

– порушення доступності (блокування) інформації;

– заперечення автентичності інформації;

– нав'язування неправдивої інформації.

Розглянемо класифікацію джерел загроз.

Носіями загроз безпеці інформації є джерела загроз. Як джерела загроз можуть виступати як суб'єкти (особистість) так і об'єктивні прояви. Причому, джерела загроз можуть перебувати як усередині захищається організації - внутрішні джерела, так і поза нею - зовнішні джерела. Розподіл джерел на суб'єктивні та об'єктивні виправдано виходячи з попередніх міркувань з приводу провини або ризику збитків інформації. А поділ на внутрішні і зовнішні джерела виправдано тому, що для однієї і тієї ж загрози методи парирування для зовнішніх і внутрішніх джерел можу бути різними.

Всі джерела загроз безпеці інформації можна розділити на три основні групи:

– обумовлені діями суб'єкта (антропогенні джерела загроз).

– обумовлені технічними засобами (техногенні джерела небезпеки).

– обумовлені стихійними джерелами.

Розглянемо антропогенні джерела загроз.

Антропогенними джерелами загроз безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочину. Тільки в

цьому випадку можна говорити про заподіяння збитку. Ця група найбільш обширна і представляє найбільший інтерес з точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватних заходів. Методи протидії в цьому випадку керовані і безпосередньо залежать від волі організаторів захисту інформації.

Як антропогенного джерела загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами захищається. Суб'єкти (джерела), дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішні, так і внутрішні.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться:

– кримінальні структури;

– потенційні злочинці і хакери;

– несумлінні партнери;

– технічний персонал постачальників телематичних послуг;

– представники наглядових організацій і аварійних служб;

– представники силових структур.

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих фахівців в області розробки і експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою вирішуваних завдань, структурою та основними функціями і принципами роботи програмно – апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

Розглянемо техногенні джерел загроз.

Друга група містить джерела загроз, які визначаються технократичної діяльністю людини і розвитком цивілізації. Однак, наслідки, спричинені такою діяльністю вийшли з під контролю людини і існують самі по собі. Ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги.

Даний клас джерел загроз безпеці інформації є особливо актуальним в сучасних умовах, так як в умовах, що склалися експерти очікують різкого зростання числа техногенних катастроф, викликаних фізичним і моральним старінням технічного парку використовуваного обладнання, а також відсутністю матеріальних засобів на його оновлення.

Технічні засоби, які є джерелами потенційних загроз безпеки інформації так само можуть бути зовнішніми і внутрішніми :

Розглянемо стихійні джерела загроз.

Третя група джерел загроз об'єднує, обставини, що становлять непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. В законодавстві і договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або запобігти або можливо передбачити, але неможливо запобігти при сучасному рівні людського знання і можливостей.

Такі джерела загроз абсолютно не піддаються прогнозування і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці як правило є зовнішніми по відношенню до захищається і під ними розуміються насамперед природні катаклізми :

– пожежі;
– землетрусу;
– повені;
– урагани;
– різні непередбачені обставини;
– незрозумілі явища;
– інші форс-мажорні обставини

Всі джерела погроз мають різну ступінь небезпеки ($К_{оп}$) і, яку можна кількісно оцінити, провівши їх ранжування. При цьому, оцінка ступеня небезпеки проводиться за непрямими показниками. В якості критеріїв порівняння (показників) можна, наприклад, вибрати:

– можливість виникнення джерела (К1) і - визначає ступінь доступності до захищуваного об’єкта (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел) або особливості обстановки (для випадкових джерел).

– готовність джерела (К2) і - визначає ступінь кваліфікації і привабливість здійснення діянь з боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних і стихійних джерел).

– фатальність (К3) і - визначає ступінь непереборності наслідків реалізації загрози.

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному обсягу впливу оцінюваного показника на небезпеку використання джерела, а 5 - максимальної.

$К_{оп}$ і для окремого джерела можна визначити як відношення добутків вищенаведених показників до максимального значення

Результати проведеного ранжирування щодо конкретного об'єкта захисту можна звести в таблицю, що дозволяє визначити найбільш небезпечні для даного об'єкта джерела загроз безпеці інформації.

При виборі допустимого рівня джерела загроз, передбачається, що джерела загроз, що мають коефіцієнт (Коп) менше (0,1 ... 0,2) можуть надалі не враховуватися, як малоймовірні. В таблиці 2.10 показано аналіз загроз ТОВ «Аквамарин».

Таблиця 2.10 – Аналіз загроз

Джерело загрози	Загроза	К1	К2	К3	Коп
Антропогенні зовнішні					
Кримінальні структури	розкрадання (копіювання) інформації	1	2	2	<0.1
	знищення інформації	1	3	2	0.1
	модифікація (спотворення) інформації	1	3	2	0.1
	порушення доступності інформації	1	1	2	<0.1

Продовження таблиці 2.10

Джерело загрози	Загроза	К1	К2	К3	Коп
	нав'язування неправдивої інформації	1	3	3	0.1
Потенційні злочинці і хакери	розкрадання (копіювання) інформації	3	4	4	0.4
	знищення інформації	2	2	3	0.1
	модифікація (спотворення) інформації	2	3	3	0.1
	порушення доступності інформації	2	3	3	0.1
	нав'язування неправдивої інформації	2	2	2	0.1
Недобросовісні партнери	розкрадання (копіювання) інформації	3	4	4	0.4
	знищення інформації	2	2	3	0.1
	модифікація (спотворення) інформації	1	2	3	0.1
	порушення доступності інформації	2	2	2	0.1
	нав'язування неправдивої інформації	2	2	2	0.1
Антропогенні внутрішні					
основний персонал (Фахівці з обслуговування комп'ютерної техніки)	розкрадання (копіювання) інформації	3	2	2	0.1
	знищення інформації	2	2	3	0.1
	модифікація (спотворення) інформації	3	2	3	0.1
	порушення доступності інформації	1	3	2	0.1
	нав'язування неправдивої інформації	4	2	2	0.1
Персонал з підвищеним рівнем доступу (Директор,	розкрадання (копіювання) інформації	2	2	2	0.1
	знищення інформації	5	3	3	0.4

Продовження таблиці 2.10

Джерело загрози	Загроза	К1	К2	К3	Коп
бухгалтер)	модифікація (спотворення) інформації	5	3	3	0.4
	порушення доступності інформації	1	2	2	<0.1
	нав'язування неправдивої інформації	5	3	3	0.4
інший персонал (Прибиральниця)	розкрадання (копіювання) інформації	2	2	2	0.1
	знищення інформації	4	2	5	0.3
	модифікація (спотворення) інформації	1	1	5	<0.1
	порушення доступності інформації	3	2	2	0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Техногенні зовнішні					
Мережі інженерних комунікації	розкрадання (копіювання) інформації	3	2	3	0.1
	знищення інформації	2	2	2	0.1
	модифікація (спотворення) інформації	3	2	3	0.1
	порушення доступності інформації	3	3	3	0.2
	нав'язування неправдивої інформації	1	1	1	<0.1
Засоби зв'язку	розкрадання (копіювання) інформації	4	4	4	0.5
	знищення інформації	2	2	3	0.1
	модифікація (спотворення) інформації	2	2	2	0.1
	порушення доступності інформації	2	2	2	0.1
	нав'язування неправдивої інформації	2	2	2	<0.1
Техногенні внутрішні					
Неякісні технічні засоби обробки	розкрадання (копіювання) інформації	3	2	3	0.1
	знищення інформації	2	2	3	0.1

Продовження таблиці 2.10

Джерело загрози	Загроза	К1	К2	К3	Коп
інформації	модифікація (спотворення) інформації	3	2	3	0.1
	порушення доступності інформації	3	3	3	0.3
	нав'язування неправдивої інформації	2	2	2	<0.1
Неякісні програмні засоби обробки інформації;	розкрадання (копіювання) інформації	3	3	3	0.3
	знищення інформації	2	2	2	<0.1
	модифікація (спотворення) інформації	3	2	3	0.1
	порушення доступності інформації	4	2	2	0.2
	нав'язування неправдивої інформації	3	3	2	0.1
Стихійні					
Пожежа		4	4	4	0.5
Землетрус		2	2	2	0.1
		2	3	4	5
Повінь		1	1	4	<0.1
Ураган		1	1	3	<0.1
Інші надзвичайні обставини		1	1	1	<0.1

Розглянемо модель порушника у ТОВ «Аквамарин».

Порушники бувають внутрішні (ті, що працюють в організації) та зовнішні. Порушниками можуть бути:

– співробітники агентства;

– кур’єри, представники від клієнтів;

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

– персонал, що обслуговує комунікації (наприклад, Internet, лінії телефонного зв'язку);

Модель порушника показана в таблиці 2.11

Таблиця 2.11 – Модель порушника

№п/п	Джерело загрози	Загрози			Інформація, яка зазнає впливу від джерел загроз
		К	Д	Ц	
1	2	3	4	5	6
1	Директор	+	+	+	Персональні дані співробітників компанії; дані про рівень заробітної плати співробітників;
2				+	Персональні дані співробітників компанії; дані про рівень заробітної плати співробітників;
				+	Зміст та перелік договорів; вартість та ціни обслуговування клієнтів; відомості про сплачення податків і зборів;
3	Бухгалтер	+	+	+	Персональні дані співробітників; дані про рівень заробітної плати співробітників;

Продовження таблиці 2.11

1	2	3	4	5	6
				+	Зміст та перелік договорів; вартість та ціни обслуговування клієнтів; відомості про сплачення податків і зборів;
4	Спеціалісти з обслуговування комп'ютерної техніки(2)			+	Зміст та перелік договорів; вартість та ціни обслуговування клієнтів; відомості про сплачення податків і зборів;
5	Хакери	+	+	+	Персональні дані співробітників; дані про рівень заробітної плати співробітників;
6	Недобросовісні партнери	+	+	+	Персональні дані співробітників; дані про рівень заробітної плати співробітників;
7	Технічний персонал постачальників послуг	+	+	+	Персональні дані півробітників; дані про рівень заробітної плати співробітників;
8	Представники наглядових організацій і аварійних служб	+	+	+	Персональні дані півробітників; дані про рівень заробітної плати співробітників;

Продовження таблиці 2.11

1	2	3	4	5	6
9	Представники силових структур	+	+	+	Персональні дані півробітників; дані про рівень заробітної плати співробітників;

Оцінимо ризики за двома факторами.

У таблиці 2.12 можна наочно відобразити зв'язок факторів негативного впливу (показників ресурсів) і ймовірностей реалізації загрози .На першому кроці оцінюється негативний вплив (показник ресурсу) за заздалегідь визначеною шкалою, наприклад від 1 до 5, для кожного ресурсу, яким загрожує небезпека.

На другому кроці по заздалегідь заданій шкалі, наприклад від 1 до 5, оцінюється ймовірність реалізації кожної загрози.

На третьому кроці обчислюється показник ризику. У найпростішому варіанті методики це робиться шляхом множення (b x c). Однак необхідно пам'ятати, що операція множення визначена для кількісних шкал. Відповідно, повинна бути розроблена методика оцінювання показників ризиків стосовно організації.

Таблиця 2.12 – Оцінка ризиків

Загроза	Показник негативного впливу (ресурсу).	Можливість реалізації загрози (суб'єктивна оцінка)	Показник ризику	Ранг ризику
Розкрадання (копіювання) інформації	2	2	4	2
Знищення інформації	2	2	4	2
Модифікація (спотворення) інформації	3	3	9	3
Порушення доступності інформації;	3	3	9	3
Нав'язування неправдивої інформації	2	3	6	3

В таблиці позначено:

Показник ризику:

Від 1-2 – низький;

Від 3-5 – середній;

Від 6-9 – високий;

Ранг ризику:

1 ранг – низький;

2 ранг – середній;

3 ранг – високий;

2.4 Обґрунтування створення КСЗІ

Проаналізувавши об’єкт інформаційної діяльності, його характеристику, розробивши модель загроз та порушників було обрано стандартний функціональний профіль захищеності 3. КЦД.1.

Призначений для АС 3 класу з підвищеними вимогами до конфіденційності, цілісності доступності:

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 }

Опишемо критерії захищеності.

КД-2. Базова довірча конфіденційність:

– політика довірчої конфіденційності, що реалізується комплексами засобами захисту , повинна визначати множину об'єктів комп’ютерної системи, до яких вона відноситься;

– комплексі засоби захисту повинні здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– комплекс засобів захисту повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

– комплекс засобів захисту повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

КО-1. Повторне використання об'єктів:

– політика повторного використання об'єктів, що реалізується комплексом засобів захисту, повинна відноситись до всіх об'єктів комп’ютерної системи;

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

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

КВ-1. Мінімальна конфіденційність при обміні:

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

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

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

ЦД-1. Мінімальна довірча цілісність:

– політика довірчої цілісності, що реалізується комплексом засобів захисту, повинна визначати множину об'єктів КС, до яких вона відноситься;

– комплекс засобів захисту повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися комплексом засобів захисту на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– комплекс засобів захисту повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО-1. Обмежений відкат:

– політика відкату, що реалізується комплексом засобів захисту, повинна визначати множину об'єктів КС, до яких вона відноситься;

– повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-1: Мінімальна цілісність при обміні:

– політика цілісності при обміні, що реалізується комплексом засобів захисту, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– комплексом засобів захисту повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання.

ДР-1. Квоти:

– політика використання ресурсів, що реалізується комплексом засобів захисту, повинна визначати множину об'єктів комп'ютерної системи, до яких вона відноситься;

– політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу;

– запити на зміну встановлених обмежень повинні оброблятися комплексом засобів захисту тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1. Ручне відновлення:

– політика відновлення, що реалізується комплексом засобів захисту, повинна визначати множину типів відмов комп'ютерної системи і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція комп'ютерної системи;

– після відмови комп'ютерної системи або переривання обслуговування комплексом засобів захисту повинен перевести комп'ютерну до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження;

– повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути комп'ютерну систему до нормального функціонування.

НР-2. Захищений журнал:

– політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються;

– КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки;

– журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події;

– КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування;

– адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація:

– політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для

використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ;

– перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму;

– КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал:

– політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ;

– достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів:

– політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції;

– політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки функції, які необхідні для виконання даної ролі;

– користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЦ-2. КЗЗ з гарантованою цілісністю:

– політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів;

– КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування;

– повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті:

– політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ;

– КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НВ-1: Автентифікація вузла:

– політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ;

– КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму;

– підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Існуюча система безпеки не реалізує одразу декілька критеріїв профілю захищеності:

Розглянемо критерії цілісності.

ЦВ-1: Мінімальна цілісність при обміні.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Критерії спостереженості:

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 (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжуються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

НО-2. Розподіл обов'язків спеціаліста з обслуговування комп'ютерної техніки

Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для спеціаліста з обслуговування комп'ютерної техніки і звичайного користувача (рівень НО-1).

Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі специфічними наборами адміністративних обов'язків. Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів). Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі.

НВ-1: Автентифікація вузла

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. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Згідно Закону України «Про захист інформації» в ІКС ТОВ «Аквамарин» оброблюється і зберігається інформація з обмеженим доступом.

Згідно Законів України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про захист персональних даних» порядок

доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Власник інформації та інформаційної системи сам може визначити необхідність створення КСЗІ та КЗЗ, якщо це не суперечить чинному законодавству.

Створення КСЗІ включає в себе створення КТЗІ та КЗЗ. Під час аналізу стану захищеності ТОВ «Аквамарин» КТЗІ відповів всім вимогам (на вході в приміщення встановлений кодовий замок, стіни, вікна та двері екрановані тощо). А при аналізі КЗЗ, були виявленні недоліки – КЗЗ не задовольнив вимоги обраного стандартного профілю захищеності. Тому в дипломній роботі увага буде приділена КЗЗ та розробці політики безпеки, як частині побудови КСЗІ.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» у ТОВ «Аквамарин» АС відносяться до третього класу, оскільки представляє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Передача інформації здійснюється через незахищене середовище. Комплексна система захисту інформації (КСЗІ) – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС .

Комплекс технічного захисту інформації (КТЗІ) – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку ІзОД технічними каналами на об’єктах інформаційної діяльності .

Для забезпечення безпеки інформації під час її обробки в АС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу АС.

Комплекс засобів захисту (КЗЗ) – сукупність всіх програмно-апаратних засобів, задіяних під час реалізації політики безпеки .

Політика безпеки (ПБ) – набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації .

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» на ТОВ «Аквамарин» циркулює інформація з обмеженим доступом(персональні данні співробітників), вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю та конфіденційна інформація вимога щодо захисту якої встановлюється її власником. Така інформація повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством . Тобто, перед створенням КСЗІ, треба визначити чи є на підприємстві інформація, яка підлягає захисту.

До організаційних заходів КСЗІ можна віднести:

– складання посадових інструкцій для користувачів та обслуговуючого персоналу;

– створення правил адміністрування системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікація користувачів;

– розробка порядку дій у випадках виявлення спроб НСД до ІС або виходу з ладу засобів захисту інформації;

– навчання користувачів правилам інформаційної безпеки.

– вибір інженерно – технічних заходів КСЗІ залежить від рівня захисту інформації. До них можна віднести:

– програмно-апаратні засоби захисту;

– розмежування потоків інформації між сегментами мережі;

– засоби шифрування і захисту від НСД;

Розглянемо СКУД та охоронно-пожежну сигналізацію.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

2.5 Розробка політики безпеки

Політика інформаційної безпеки є планом високого рівня, в якому описуються цілі і завдання заходів у сфері безпеки. Політика описує безпеку в узагальнених термінах, без специфічних деталей і не оперує способами реалізації.

Перш ніж приступати до розробки керівних документів, необхідно визначити глобальні цілі політики підприємства та створити концепцію.

Призначення політики інформаційної безпеки:

– збереження конфіденційності критичних інформаційних ресурсів;

– забезпечення безперервності доступу до інформаційних ресурсів підприємства для підтримки бізнес діяльності;

– захист цілісності і доступності ділової інформації з метою підтримки можливості підприємства по наданню послуг високої якості і ухваленню ефективних управлінських рішень;

– підвищення обізнаності користувачів в області ризиків, пов'язаних з інформаційними ресурсами підприємства;

– визначення міри відповідальності і обов'язків співробітників по забезпеченню інформаційної безпеки в Компанії.

Розглянемо призначення документа політики безпеки

Політика встановлює структуру захисту інформації з обмеженим доступом, сфери відповідальності користувачів та адміністраторів, мети, завдання і функції користувачів та адміністраторів.

Метою діяльності по забезпеченню інформаційної безпеки є зниження погроз інформаційній безпеці до прийнятного рівня. Основні завдання діяльності по забезпеченню інформаційної безпеки:

• виявлення потенційних погроз інформаційній безпеці;

• запобігання інцидентам інформаційної безпеки;

• виключення або мінімізація виявлених погроз.

Доступ і періодичність внесення змін: документ розроблений для внутрішнього користування співробітників.

Періодичність перегляду документу – 1 раз на рік.

Розглянемо терміни та визначення політики безпеки.

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[3].

Автоматизована система (далі АС) — організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.[3]

Інформаційна система (далі ІС) — сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.[3]

Інформація з обмеженим доступом — конфіденційна, таємна та службова інформація[3].

Політика безпеки інформації — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації[3].

Загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС[3].

Безпека інформації — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації[3].

Захист інформації в АС — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз[3].

Користувач — фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

Несанкціонований доступ до інформації; НСД до інформації — доступ до інформації, здійснюваний з порушенням ПРД.

Розмежування доступу — сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

Адміністратор безпеки — адміністратор, відповідальний за дотримання політики безпеки.

Порушник — користувач, який здійснює несанкціонований доступ до інформації[3].

Втрата інформації — неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

Комп'ютерний вірус — програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки[3].

Модель загроз — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз[3].

Модель порушника — абстрактний формалізований або неформалізований опис порушника[3].

Ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Автентифікація — процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.[3].

Пароль — секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.[3].

Розглянемо призначення та правову основу документа політики безпеки.

Політика інформаційної безпеки ТОВ "Аквамарин" (далі – Політика) визначає систему поглядів на проблему забезпечення безпеки інформації і є систематизованим викладом цілей і завдань захисту, як одне або декілька правил, процедур, практичних прийомів і керівних принципів в області інформаційної безпеки, якими необхідно керуватися в своїй діяльності, а також основних

принципів побудови, організаційних, технологічних і процедурних аспектів забезпечення безпеки інформації.

Політика враховує сучасний стан і найближчі перспективи розвитку інформаційних технологій у ТОВ "Аквамарин", цілі, завдання і правові основи їх експлуатації, режими функціонування, а також містить аналіз погроз безпеці для об'єктів і суб'єктів інформаційних стосунків ТОВ "Аквамарин".

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

Дана політика безпеки розроблена на базі нормативних документів:

– Закон України «Про інформацію»;

– Закон України «Про захист персональних даних»;

– Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

– НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

– НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

– ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації;

– ISO/IEC 17799 - Практичні правила менеджменту інформаційної безпеки.

Розглянемо правила політики безпеки контролю доступу до приміщень організації.

Правила для будівлі в цілому:

– на підприємстві має бути встановлена система відеоспостереження;

– система відеоспостереження повинна охоплювати як зовнішній периметр, так і внутрішні приміщення будівлі;

– система відеоспостереження за внутрішніми приміщеннями може охоплювати лише коридор і важливі приміщення (серверна);

– можливість потрапити до будівлі, минувши КПП, має бути повністю відсутня;

– при винесенні технічних засобів, що належать підприємству, необхідно надати дозвіл на КПП;

– всі приміщення мають бути обладнані засобами пожежогасіння.

– Робота технічних засобів залежить від безлічі чинників. Особливо від електричної мережі. Перебої живлення можуть порушити процес обробки даних.

Правила для всіх приміщень тих, що мають засоби обробки інформації:

– необхідне забезпечення стабілізованим живленням кожного компонента інформаційної системи;

–необхідні резервні джерела живлення для устаткування;

– робочі місця повинні розташовуватися відповідно до санітарних норм (не менше 4,5м2 виробничої площі).

Розглянемо правила політики безпеки для апаратних засобів

Апаратні засоби є частиною звороту інформації і є інформаційним ресурсом. Збереження належної якісної роботи – одне з пріоритетних завдань політики безпеки підприємства.

– кожен апаратний засіб підлягає інвентаризаційному обліку, відповідно документам;

– необхідно скласти номенклатуру по всьому устаткуванню з вказівкою місця його розміщення;

– суворо дотримуватися правил експлуатації устаткування;

– купувати устаткування лише у надійних постачальників, що дають гарантію і що мають власні центри обслуговування в межах локації підприємства;

– ремонтувати апаратне забезпечення лише у організацій, що мають ліцензію на роботу з засобами захисту інформації;

– при заміні устаткування або ремонті, переконатися, що конфіденційні дані видалені з носія, маючи відповідну копію з цими даними;

– регулярно проводити діагностику апаратних засобів.

Локальна обчислювальна мережа – величезна сполучна ланка передачі даних між користувачами. Завдання – забезпечити стабільність і якість роботи мережі, безпеку передачі даних по ній.

Правила для локальної обчислювальної мережі:

– має бути забезпечений резерв вільних локацій при підключенні нової робочої станції. Все повинно відбуватися без порушення роботи мережі;

– забезпечити безпеку ЛВС шляхом обмеження доступу до мережевого устаткування.

Розглянемо правила політики безпеки для програмних засобів.

Програмне забезпечення впливає на швидкість і якість обробки даних. Також тип ПЗ залежить від типу передаваної інформації. Слід уважно вибирати ПЗ для підприємства. Не дотримання цього правила може привести до втрати даних, зайвим витратам на встановлення нового ПЗ, втрати інформації.

– програмне забезпечення, використовуване на підприємстві, а також документація, що поставляється з ним, мають бути враховані;

– на ПК повинно встановлюватися ліцензійне ПЗ, або ПЗ ,яке не порушує авторських прав;

– при установці ПЗ необхідно враховувати політику інформаційної безпеки підприємства;

– встановлення устаткування повинна виробляти спеціально вивчена людина;

– перед встановленням ПЗ повинно бути протестовано;

– перед початком використання ПЗ, співробітників необхідно навчити правильному використанню;

– кожен користувач повинен знати, відповідно до договору, які права інтелектуальної власності він може порушити;

– стежити за оновленнями і встановлювати їх (виконується відповідальними за це особами);

– використовувати програмний засіб може особа, що має на це права;

– по можливості забезпечити оптимальні умови для роботи устаткування;

– захист програмних засобів ведеться як від помилок програм, так і від помилок користувача.

Резервування і архівація – надійні способи зберігання інформації. Варто уважно прослідити яким саме чином буде проходити резервування даних. Забезпечити якість і збереження архівної інформації.

При використанні певних програмних засобів (бази даних, файловий сервер і так далі) слід передбачити автоматичне резервування даних на окремому носієві.

Зберігання даних повинне не залежати від системи. Запис резервованих даних повинен вестися на окремих машинах. Слід передбачити резервне джерело живлення для виключення непереборних ситуацій не пов'язаних з виробництвом. У міру запису даних повинна вестися їх архівація.

Термін зберігання інформації призначається на вимогу керівника і відповідно до документації. Зберігати дані можна в окремому приміщенні, так і в спеціально відведеному місці. В разі підприємства місце для зберігання архівних даних є (невелике приміщення без вікон).

Необхідно призначити відповідального за архівом, який поповнюватиме дані, а також тестувати носії на придатність і якість після часу. Також варто призначити відповідального за утилізацію або видалення даних по закінченню терміну давності.

Утилізація повинна супроводжуватися повним видаленням даних з носія, лише після цього варто утилізувати сам носій вже без будь-якої інформації, що належить підприємству.

Доступ до резервування, архівації, зберігання, утилізації даних мають лише спеціальних осіб, що мають на це допуск.

Розглянемо правила для політики безпеки управління доступом.

Суворе розділення повноважень і можливостей співробітників допомагає уникнути несанкціонованого доступу до різної інформації. Сучасні методи допомагають це зробити фізично. При здобутті даних спочатку потрібно пройті реєстрацію з позитивною ідентифікацією.

– для кожної посади мають бути визначені повноваження, і доступна лише та інформація, яка йому необхідна, повинен вестися облік даних, які отримав працівник;

– ключі від приміщень видаються особам, що мають права доступу, при цьому заноситься відповідний запис в журнал;

– кількість символів в паролі має бути не менше ніж вісім, бути таким, що діє протягом 60 днів після останньої зміни;

– пароль повинен періодично мінятися для всіх співробітників підприємства. Використання старих паролів не дозволяється;

– дані про логіни і паролі повинні зберігатися централізовано;

– передача логіна або пароля іншій особі заборонена;

– для осіб, що мають доступ до секретних документів призначити надійніший пароль, що виключає доступність і простоту підбору (ім'я, прізвище і так далі);

– одночасне використання одного логіна на декількох станціях неможливе;

– при тривалій відсутності користувача або звільненні, його обліковий запис видаляється, робоча станція роз-реєструється;

– при введенні пароля в програмних засобах або передачі його через ЛВС, пароль не повинен відображуватися в явному вигляді;

– створити правило обмеження числа сеансів. Після закінчення заданого проміжку часу – автоматичний вихід з системи. Для деяких непередбачених ситуацій передбачити можливість збільшення часу знаходження в системі;

– при установці нових програмних засобів слід отримати право на це, відповідне правилам безпеки.

Розглянемо правила безпеки антивірусної системи

Антивіруси – потужна зброя з шкідливими програмами. Вони завжди мають бути активними, щоб у будь-який момент захистити програму/мережу/дані від атаки. Будь-які порушення ходу роботи антивірусу можуть привести до зараження машини і знищення інформації.

– на всіх призначених для користувача системах ще до того, як вони будуть підключені до мережі, слід встановити програмне забезпечення для захисту від вірусів;

– користувачі повинні сприяти оновленню цього програмного забезпечення, а також не повинні відключати ці засоби;

– користувачі не повинні відключати антивірусне програмне забезпечення при запуску завантажуваного з Internet в систему користувача програмного забезпечення;

– користувачі, які завантажують будь-які дані або програми із зовнішнього носія, повинні перед завантаженням сканувати цей носій на предмет наявності на ньому вірусів;

– всі системи, підключені до мережі організації, повинні піддаватися періодичній загальній перевірці на шкідливі програми. Перевірки повинні проходить не рідше за один раз в місяць.

Розглянемо правила політики безпеки зовнішнього доступу.

Інтернет – одна з невід'ємних частин нашого життя. Використання Інтернету надає безліч переваг, але тут є і «підводні камені». Величезній загрозі піддається підприємство при використанні Інтернету. Варто захищати ПЗ додатковими модулями для запобігання вторгненню, атаці, просочуванню інформації.

– розробити правила під'єднання до мережі Інтернет;

– проводити регулярне обслуговування для підтримки порядку в загальнодоступних даних;

– системні адміністратори несуть відповідальність за процедури обслуговування серверів, що надають інформацію або послуги користувачам Інтернет;

– користувачі, що мають доступ до Інтернет, повинні заздалегідь пройти програму вчення, де буде роз'яснена політика компанії у сфері безпеки і відповідальність користувачів за представлення компанії в світовій мережі;

– користувачі не повинні пересилати жодної інформації, яка може завдати збитку репутації організації або їх особистої;

– користувачі можуть завантажувати програмне забезпечення Інтернет, яке допоможе їм виконувати свої функції в організації тільки після узгодження з системним адміністратором;

– організація повинна зберегти за собою право блокування доступу до всіх сайтів, які вважаються неприйнятними, а також робити реєстраційні записи про відвідини сайтів всіма користувачами, на підставі яких у будь-який час можна провести аудиторську перевірку;

– адміністратор безпеки повинен розробити архітектуру системи електронної пошти так, щоб забезпечити належну доставку повідомлень як усередині організації, так і в Інтернет. Використання посередницьких програм допускається;

– організація повинна зберігати і архівувати всі повідомлення електронної пошти, які проходять через її сервер. Архів повинен зберігатися на включеному в мережу пристрої, що запам'ятовує;

– адміністратори повинні переносити повідомлення, що архівуються, на автономний пристрій, що запам'ятовує, кожні шість місяців, видаляючи ці повідомлення з оперативних пристроїв, що запам'ятовують. Після закінчення терміну придатності даних, інформація повністю стирається з носіїв без можливості відновлення;

– організація має право сканувати вміст кожного повідомлення електронної пошти, яке проходить через її сервери, на основі заздалегідь встановлених критеріїв. Якщо повідомлення не відповідає критеріям, то воно не повинне доставлятися користувачеві;

– розмір повідомлень електронної пошти, що відправляються і отримуваних користувачами, в цілому, не повинен перевищувати встановленого ліміту. Всі останні випадки обговорюються з адміністратором;

– правило обміну конфіденційною інформацією включає розпорядження шифрувати повідомлення перед їх пересилкою і "підписувати" їх цифровими підписами;

– користувачі не повинні брати участь в розсилці шкідливих послань, що пересилаються по ланцюжку, містять погрози.

Розглянемо відповідальність за дотримання положень Політики безпеки.

Категорично заборонена будь-яка поведінка, яка несприятливо відбивається на роботі інших осіб в системах і мережах організації, або яка може нашкодити іншим особам.

Керівництво залишає за собою право досліджувати дані, що зберігаються на всіх комп'ютерах і в мережевих системах, за допомогою засобів фізичного дослідження і електронного моніторингу. Якщо в зібраній інформації виявлені факти порушення правил інформаційної безпеки або закону, то організація може використовувати ці дані для дисциплінарних стягнень або правових санкцій.

Керівництво має право розірвати контракти і договори з підрядчиками і іншими зовнішніми користувачами, якщо вони порушують розпорядження правив

або демонструють поведінку, яка заважає нормальній роботі мережі і комп'ютерних систем підприємства.

Розглянемо контроль за дотриманням положень Політики безпеки.

Поточний контроль дотримання Політики здійснює адміністратор безпеки. Контроль здійснюється шляхом проведення моніторингу і менеджменту інцидентів інформаційної безпеки організації, за результатами оцінки інформаційної безпеки, а також в рамках інших контрольних заходів.

Політика оговорює відповідальність за дотримання положень відповідної Політики. Обумовлює контроль за дотримання положень відповідної Політики.

Політика безпеки підприємства розвивається і іншими документами підприємства, та пристосовується до вимог чинного законодавства.

Політику доповнено інструкціями для користувачів інформаційної системи.

До Політики додається наказ, який створено новий структурний підрозділ – відділ інформаційної безпеки. Штат відділу складається з однієї особи – адміністратора безпеки.

До Політики додаються інструкції:

- адміністратора безпеки, що визначає обов'язки, права і відповідальність адміністратора інформаційної безпеки;
- користувача інформаційної системи персональних даних, що визначає загальні функції, права і обов'язки користувача при підготовці і обробки персональних даних на ПК, що входять до складу інформаційної системи персональних даних.

Товариство з обмеженою відповідальністю «Аквамарин»

НАКАЗ

--.--.-- м. Дніпро №001

Про запровадження суміщення посад

ДОРУЧИТИ:

ПІБ., спеціалісту з обслуговування комп'ютерної техніки, без увільнення його від основної роботи, обумовленої політики безпеки, виконання додаткової роботи на суміщення за посадою адміністратора безпеки зі щомісячною доплатою у розмірі 40% посадового окладу вакантної посади адміністратора безпеки, із --.--.--.

Підстави: 1.Заява ПІБ від --.--.--, зареєстрована за № 0026.

Директор

Розглянемо посадову інструкцію адміністратора безпеки.

Адміністратор безпеки має такі загальні положення:

– інструкція визначає функції, права і обов'язки адміністратора безпеки інформації по питаннях забезпечення інформаційної безпеки при роботі з інформаційною системою;

– адміністратор безпеки інформації призначається з числа співробітників і забезпечує правильність використання і нормальне функціонування встановлених систем захисту інформації від НСД, резервне копіювання інформації, оновлення антивірусних баз, робить періодичний аналіз захищеності;

– справжня інструкція є доповненням до нормативних документів, що діють, по питаннях забезпечення безпеки інформації з обмеженим доступом, і не виключає обов'язкового виконання їх вимог;

Основні функції адміністратора безпеки інформації:

– контроль за виконанням вимог нормативних документів, що діють, в питаннях забезпечення захисту інформації з обмеженим доступом, що оброблюється в інформаційній системі;

– налаштування і супровід в процесі експлуатації системи управління доступом в інформацій системи обробки інформації з обмеженим доступом;

– контроль доступу осіб в приміщення, де встановлені АС відповідно до списку співробітників, допущених до роботи на АС;

– Контроль за своєчасним проведенням зміни паролів для доступу до АС користувачами відповідних АС;

Адміністратор безпеки інформації має право:

– брати участь в аналізі ситуацій, що стосуються функціонування засобів захисту інформації і розслідування фактів несанкціонованого доступу;

– вимагати припинення обробки інформації з обмеженим доступом в разі порушення встановленого порядку робіт або порушення функціонування засобів і систем захисту інформації;

Розглянемо посадову інструкцію директора.

Директор має такі загальні положення:

– Директор підприємства належить до професійної групи «Керівники» ;

– Призначення на посаду керівника підприємства та звільнення з неї здійснюється з дотриманням вимог Кодексу законів про працю України та чинного законодавства про працю;

– Директор підприємства є підзвітним засновникам підприємства в особі __ ;

Директор має такі завдання та обов'язки:

– визначає, формулює, планує, здійснює і координує всі види діяльності підприємства;

– визначає напрями розвитку підприємства у формуванні цінової, кредитно-банківської, податкової та страхової політики, соціальної та зовнішньоекономічної діяльності;

– організує роботу і ефективну взаємодію виробничих одиниць, цехів та інших структурних підрозділів підприємства, направляє їх діяльність на досягнення високих темпів розвитку і удосконалення виробництва та продукції;

– забезпечує відповідність продукції кращим світовим зразкам з метою задоволення потреб замовників і споживачів у відповідних видах продукції, підвищення продуктивності праці, ефективності виробництва і якості продукції на основі широкого запровадження нової техніки і прогресивної технології, організації праці, виробництва і управління, удосконалення господарського механізму;

– направляє діяльність персоналу на досягнення високих економічних та фінансових результатів;

– забезпечує виконання підприємством програми оновлення продукції, планів капітального будівництва, обов'язків перед державним бюджетом, постачальниками, замовниками і банками;

– організує виробничо-господарську діяльність підприємства на основі застосування методів обґрунтованого планування, нормативних матеріалів, фінансових і трудових витрат, широкого розповсюдження передового досвіду, а також максимальної мобілізації резервів виробництва шляхом досягнення високих техніко-економічних показників, підвищення технічного рівня і якості продукції, раціонального і економного витрачання всіх видів ресурсів;

– здійснює заходи з соціального розвитку колективу підприємства, забезпечує розроблення, укладання і виконання колективного договору, проводить роботу щодо зміцнення трудової і виробничої дисципліни.Забезпечує сполучення економічних і адміністративних методів керівництва, матеріальних і моральних стимулів підвищення ефективності виробництва, а також підсилення відповідальності кожного працівника за доручену йому справу;

– вирішує всі питання в межах наданих йому прав, доручає виконання окремих організаційно-господарських функцій іншим посадовим особам: заступникам керівника, керівникам виробничих підрозділів підприємства;

– забезпечує додержання законності, активне використання правових засобів удосконалення управління, зміцнення договірної дисципліни і обліку, господарського розрахунку;

– здійснює заходи щодо соціального захисту колективу підприємства, забезпечення і збереження зайнятості працівників;

– представляє підприємство в органах державної влади і у взаємовідносинах з партнерами;

Розглянемо права директора на підприємстві.

Директор підприємства має право:

– без доручення діяти від імені підприємства;

– Представляти інтереси підприємства у взаємовідносинах з громадянами, юридичними особами та органами державної влади;

– розпоряджатися майном підприємства з дотриманням вимог, визначених законодавством, Статутом підприємства, іншими нормативними правовими актами;

– відкривати в банківських установах розрахунковий та інші рахунки;

– укладати трудові договори з працівниками;

Розглянемо посадову інструкцію спеціаліста з обслуговування комп'ютерної техніки.

Спеціаліст з обслуговування комп'ютерної техніки має такі загальні положення:

– спеціаліст з обслуговування комп'ютерної техніки приймається на роботу і звільняється наказом директора підприємства, у відповідності вимогами Кодексу законів про працю України;

– на посаду спеціаліста з обслуговування комп'ютерної техніки призначається особа, що має вищу або середньо-спеціальну освіту, та досвід роботи по обслуговуванню комп'ютерної техніки і локальної обчислювальної мережі не менше 3 років;

– спеціаліст з обслуговування комп'ютерної техніки підпорядковується безпосередньо директорові підприємства;

– у своїй роботі спеціаліст з обслуговування комп'ютерної техніки керується Конституцією України, Кодексом законів про працю України,

нормативно-правовими і законодавчими актами України, що стосуються його роботи, цією посадовою інструкцією;

– на час відсутності спеціаліста з обслуговування комп'ютерної техніки його обов'язки виконує особа, призначена директором підприємства у встановленому порядку. Дана особа набуває відповідні права і несе відповідальність за якісне і своєчасне виконання покладених на неї обов'язків;

Спеціаліст з обслуговування комп'ютерної техніки має такі завдання та обов'язки:

– забезпечувати працездатний стан комп'ютерної техніки, локальної обчислювальної мережі, операційних систем, системного і прикладного програмного забезпечення (далі – ПЗ) ;

– обслуговувати комп'ютерну техніку, проводити діагностику і профілактику з метою виявлення і усунення можливих причин виходу техніки із ладу;

– проводити установку операційних систем, системного і прикладного ПЗ, яке використовується у виробничому процесі. Видаляє все ПЗ, яке не бере участі у виробничому процесі, призводить до перекручування або знищення службової інформації;

– визначати причини відмов в роботі технічних засобів, готувати пропозиції по їх усуненню і попередженню;

– забезпечувати високу якість та надійність обладнання, що використовується, підвищувати ефективність роботи комп'ютерної техніки і оргтехніки на підприємстві;

– брати участь у формуванні бюджету на оргтехніку підприємства, оформлювати заявки на закупівлю необхідної оргтехніки, визначати необхідність закупівлі оргтехніки;

– надавати консультаційну допомогу директорові підприємства при замовленні оргтехніки, враховуючи навантаження на комп'ютерну техніку і доцільність;

– вести моніторинг руху комп'ютерної техніки на підприємстві.

Маємо такі права:

– спеціаліст з обслуговування комп'ютерної техніки має право: Знайомитися з документами, що визначають його права й обов'язки по займаній посаді, критерії оцінки якості виконання посадових обов'язків;

– брати участь в обговоренні питань щодо обов'язків, що виконуються ним;

– повідомляти безпосередньому керівнику про усі недоліки, виявлені у процесі виконання своїх посадових обов'язків та у господарській діяльності підприємства (його структурних підрозділах) і вносити пропозиції по їх усуненню;

– вимагати від безпосереднього керівника та інших посадових осіб підприємства сприяння у виконанні своїх посадових обов'язків;

– підписувати і візувати документи в межах своєї компетенції;

– вимагати від керівників структурних підрозділів підприємства інформацію і документи, необхідні для виконання своїх посадових обов'язків;

– доповідати директору підприємства про всі виявленні випадки порушень працівниками і керівниками структурних підрозділів чинного законодавства, наказів та розпоряджень керівництва підприємства;

– вносити безпосередньому керівникові пропозиції щодо удосконалення роботи, пов'язаної з виконанням обов'язків передбачених цією посадовою інструкцією;

– вимагати від директора підприємства забезпечення організаційно-технічних умов і оформлення встановлених документів, необхідних для виконання посадових обов'язків.

Розглянемо посадову інструкцію бухгалтера.

Бухгалтер має такі загальні положення:

– призначення на посаду бухгалтера та звільнення з неї здійснюється наказом директора підприємства за поданням головного бухгалтера з дотриманням вимог Кодексу законів про працю України;

– бухгалтер підпорядковується директору підприємства;

– за відсутності бухгалтера його обов'язки виконує особа, призначена у встановленому порядку), яка набуває відповідних прав та несе відповідальність за належне виконання покладених на неї обов'язків.

Бухгалтер має такі завдання та обов’язки:

– самостійно і в повному обсязі веде облік необоротних активів, запасів, коштів, розрахунків та інших активів, власного капіталу та зобов'язань, доходів та витрат за прийнятою на підприємстві формою бухгалтерського обліку з додержанням єдиних методологічних засад бухгалтерського обліку та з урахуванням особливостей діяльності підприємства й технології оброблення даних;

– забезпечує повне та достовірне відображення інформації, що міститься у прийнятих до обліку первинних документах, на рахунках бухгалтерського обліку;

– за погодженням з власником (керівником) підприємства та керівником підрозділу бухгалтерського обліку, подає в банківські установи документи для перерахування коштів згідно з визначеними податками й платежами, а також для розрахунків з іншими кредиторами відповідно до договірних зобов'язань;

– бере участь у проведенні інвентаризації активів і зобов'язань, оформленні матеріалів, пов'язаних з нестачею та відшкодуванням втрат під нестачі, крадіжки й псування активів підприємства, у перевірках стану бухгалтерського обліку у філіях, представництвах, відділеннях та інших відокремлених підрозділах підприємства;

– готує дані для включення їх до фінансової звітності, здійснює складання окремих її форм, а також форм іншої періодичної звітності, яка ґрунтується на даних бухгалтерського обліку;

– забезпечує підготовку оброблених документів, реєстрів і звітності для зберігання їх протягом установленого терміну.

Бухгалтер має право:

– ознайомлюватися з проектами рішень керівництва підприємства, що стосуються його діяльності;

– вносити на розгляд головного бухгалтера пропозиції по вдосконалення роботи, пов'язаної з обов'язками, що передбачені цією інструкцією;

– в межах своєї компетенції повідомляти безпосередньому керівнику про всі виявлені недоліки в діяльності підприємства та вносити пропозиції щодо їх усунення;

– вимагати та отримувати особисто або за дорученням головного бухгалтера у керівників структурних підрозділів та фахівців інформацію та документи, необхідні для виконання його посадових обов'язків;

– залучати фахівців усіх структурних підрозділів до виконання покладених на нього завдань;

– вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків.

Розглянемо посадову інструкцію користувача інформаційної системи персональних даних.

Користувач інформаційної системи персональних даних має такі загальні положення:

– користувач інформаційної системи персональних даних здійснює обробку персональних даних;

– користувачем є кожен співробітник, що бере участь в рамках своїх функціональних обов'язків в процесах обробки персональних даних.

– користувач несе персональну відповідальність за свої дії;

– користувач в своїй роботі керується інструкцією користувача, політикою інформаційної безпеки;

– методичне керівництво роботою користувача здійснюється адміністратором безпеки;

Користувач інформаційної системи персональних даних має такі посадові обов'язки:

– виконувати вимоги та інструкції пов’язані з забезпеченням інформаційної безпеки;

– виконувати вимоги парольної політики;

– виконувати вимоги політики безпеки зовнішнього доступу;

– звертатися з питань безпеки інформації до адміністратора безпеки, повідомляти про випадки, що можуть порушувати інформаційну безпеку.

Користувачам забороняється:

– розголошувати інформацію, що захищається, третім особам;

– копіювати інформацію, що захищається, зовнішні носії без дозволу свого керівника або адміністратора безпеки;

– самостійно встановлювати, тиражувати, або модифікувати програмне забезпечення і апаратне забезпечення, змінювати встановлений алгоритм функціонування технічних і програмних засобів;

– заборонено підключати до робочої станції інформаційної мережі особисті зовнішні носії і мобільні пристрої;

– відключати засоби захисту інформації;

– виконувати процедури не пов'язані зі службовими обов'язками.

Розглянемо організацію парольного захисту:

– пароль видається адміністратор безпеки або створюється користувачем особисто;

– пароль має змінюватися не більш ніж раз на 60 днів. кількість символів в паролі має бути не менш ніж 8;

– пароль має виключати простоту підбору;

– пароль має містити заголовні і прописні літери та цифри;

– забороняється використовувати пароль, який був використаний раніше;

– забороняється передавати дані про обліковий запис іншим співробітникам або стороннім особам;

– під час введення пароль необхідно забезпечити необхідність його перегляду іншими особами або технічними засобами;

– забороняється зберігання паролю в письмовому вигляді (на папері, електронному носії, предметах);

– забороняється робота під обліковим записом іншої особи;

– негайно повідомляти про втрату, несанкціоновану зміну паролю або строку його дії.

2.6 Аналіз ризиків після впровадження політики безпеки

Розроблені елементи політики безпеки спрямовані на зниження (перекриття) наступних ризиків:

– розкрадання (копіювання) інформації;

– знищення інформації;

– модифікація (спотворення) інформації;

– порушення доступності інформації;

– нав'язування неправдивої інформації.

які знизяться, після застосування ПБ, до першого рівня. Це підтверджується змінами аналізу загроз і порушника .

Після впровадження політики безпеки у ТОВ «Аквамарин» ризик виникнення загроз на фірмі знизився у зв'язку з розробленням політики безпеки, посадових інструкцій та додання нового структурного підрозділу інформаційної безпеки, штат співробітників яких складається з однієї людини – адміністратор безпеки інформації. Оцінку ризиків, після впровадження політики безпеки ми оцінюємо завдяки зміненими показниками аналізу загроз (таблиця 2.13) у таблиці 2.14. Завдяки запровадженій політиці безпеки показники загроз (розкрадання (копіювання) інформації, знищення інформації, модифікація (спотворення) інформації, порушення доступності інформації, нав'язування неправдивої інформації у ТОВ «Аквамарин» знизились удвічі. Це ми бачимо по таблиці 2.13.

Таблиця 2.13 – Аналіз загроз після впровадження ПБ

Джерело загрози	Загроза	К1	К2	К3	$К_{оп}$
Антропогенні зовнішні					
Кримінальні структури	розкрадання (копіювання) інформації	1	1	1	<0.1
	знищення інформації	1	2	1	<0.1
	модифікація (спотворення) інформації	1	2	1	<0.1

Продовження таблиці 2.13

1	2	3	4	5	6
	порушення доступності інформації	1	1	2	<0.1
	нав'язування неправдивої інформації	1	2	2	<0.1
Потенційні злочинці і хакери	розкрадання (копіювання) інформації	2	3	3	0.1
	знищення інформації	1	1	2	<0.1
	модифікація (спотворення) інформації	1	2	2	<0.1
	порушення доступності інформації	1	2	2	<0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Недобросовісні партнери	розкрадання (копіювання) інформації	2	3	3	0.1
	знищення інформації	1	1	2	<0.1
	модифікація (спотворення) інформації	1	1	2	<0.1
	порушення доступності інформації	1	1	1	<0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Антропогенні внутрішні					
Основний персонал (Фахівці з обслуговування комп'ютерної техніки)	розкрадання (копіювання) інформації	2	1	1	<0.1
	знищення інформації	1	1	2	<0.1
	модифікація (спотворення) інформації	2	1	2	<0.1
	порушення доступності інформації	1	2	1	<0.1
	нав'язування неправдивої інформації	3	1	1	<0.1
Персонал з підвищеним рівнем доступу (Директор, бухгалтер)	розкрадання (копіювання) інформації	1	1	1	<0.1
	знищення інформації	4	2	2	0.1
	модифікація (спотворення) інформації	4	2	2	0.1
	порушення доступності інформації	1	1	1	<0.1
	нав'язування неправдивої інформації	4	2	2	0.1
Інший персонал (Прибиральниця)	розкрадання (копіювання) інформації	1	1	1	<0.1

Продовження таблиці 2.14

1	2	3	4	5	6
	знищення інформації	3	1	4	0.1
	модифікація (спотворення) інформації	1	1	4	<0.1
	порушення доступності інформації	1	1	1	<0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Техногенні зовнішні					
Мережі інженерних комунікації	розкрадання (копіювання) інформації	2	1	2	<0.1
	знищення інформації	1	1	1	<0.1
	модифікація (спотворення) інформації	2	1	2	<0.1
	порушення доступності інформації	2	2	2	0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Засоби зв'язку	розкрадання (копіювання) інформації	3	3	3	0.2
	знищення інформації	1	1	2	<0.1
	модифікація (спотворення) інформації	1	1	1	<0.1
	порушення доступності інформації	1	1	1	<0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Техногенні внутрішні					
Неякісні технічні засоби обробки інформації	розкрадання (копіювання) інформації	2	1	2	<0.1
	знищення інформації	1	1	2	<0.1
	модифікація (спотворення) інформації	2	1	2	<0.1
	порушення доступності інформації	2	2	2	0.1
	нав'язування неправдивої інформації	1	1	1	<0.1
Неякісні програмні засоби обробки інформації;	розкрадання (копіювання) інформації	2	2	2	0.1
	знищення інформації	1	1	1	<0.1
	модифікація (спотворення) інформації	2	1	1	<0.1
	порушення доступності інформації	3	1	1	<0.1
	нав'язування неправдивої інформації	2	2	1	<0.1

Продовження таблиці 2.14

1	2	3	4	5	6
Стихійні					
	Пожежа	3	3	3	0.2
	Землетрус	1	1	1	<0.1
	Повінь	1	1	3	<0.1
	Ураган	1	1	2	<0.1
	Інші надзвичайні обставини	1	1	1	<0.1

Таблиця 2.14 – Оцінка ризиків після впровадження політики безпеки

Загроза	Показник негативного впливу (ресурсу).	Можливість реалізації загрози (суб'єктивна оцінка)	Показник ризику	Ранг ризику
Розкрадання (копіювання) інформації	2	1	2	1
Знищення інформації	2	1	2	1
Модифікація (спотворення інформації)	3	2	6	3
Порушення доступності інформації	3	2	6	3
Нав'язування неправдивої інформації	2	2	4	2

Як бачимо, показник ризику знизився вдвічі, отже, можна сказати, що розроблена політика безпеки ТОВ «Аквамарин» буде ефективна.

2.7 Висновки до другого розділу

Під час розробки другого розділу було виконано:

– обстеження об'єкта інформаційної діяльності;

– визначено і виконано категоріювання інформації, що циркулює в інформаційній системі;

– розроблено аналіз загроз та порушника;

– розроблено політику безпеки інформації для інформаційної системи.

Виконання цих задач є підтвердженням досягнення заданої мети, тобто за рахунок цих дій, вдалося забезпечити захист інформаційних ресурсів інформаційно-комунікаційної системи та розроблено політику безпеки для ТОВ «Аквамарин».

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Розрахунок капітальних витрат

Метою економічного розділу є розрахунок витрат на створення та впровадження політики безпеки інформації в ІКС підприємства.

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

Фіксовані витрати на впровадження системи розраховуватимуться за формулою:

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн.;

$К_{н}$ – витрати на встановлення та налагодження ПЗ, грн.;

$К_{зпз}$ – вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації та додаткового програмного забезпечення: резервне копіювання, контроль стану обладнання, інструктаж з ІБ, встановлення та налаштування ПЗ.

3.1.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням фаєрволу, антивірусу, налагодженням та встановленням ПЗ та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф, \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн.;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 200 грн/год.

Час на налагодження резервного копіювання займає 2 год.:

$$З = ТС* Ф = 200*2 = 400 грн.$$

Час на розробку алгоритму захисту від витоку інформації займає 5 год.:

$$З = ТС* Ф = 200*5 = 1000 грн.$$

Час на впровадження запропонованої політики безпеки займає 3 год.:

$$З = ТС* Ф = 200*3 = 600 грн.$$

Час на встановлення антивірусної програми McAfee займе 2 год.:

$$З = ТС* Ф = 200*2 = 400 грн.$$

Час на встановлення Windows 11 Pro займе 4 год.:

$$З = ТС* Ф = 200*4 = 800 грн.$$

Час на встановлення Microsoft Office 2021 займе 4 год.:

$$З = ТС* Ф = 200*4 = 800 грн.$$

3.1.2 Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується на підприємстві.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість
Резервне копіювання	Kingston USB3.2 Gen 2 DataTraveler Max (2929 грн. * 1 шт.)	2929 грн.
Антивірусний захист	McAfee Internet Security 2023 (810 грн. * 4)	3240 грн.
ОС	Windows 11 Pro (1150 грн. * 4 шт.)	4600 грн.
Пакет офісних програм	Microsoft Office 2021 Pro Plus (2000 грн. * 4 шт.)	8000 грн.

Фіксовані витрати на проєктування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 400 + 2929 = 3329 грн.$$

Розробка алгоритму захисту від витоку інформації:

К = 1000 грн.

Впровадження запропонованої політики безпеки:

К = 600 грн.

Антивірусний захист McAfee Internet Security 2023:

К = 400 + 3240 = 3640 грн.

Оновлення ОС на Windows 11 Pro:

К = 800 + 4600 = 5400 грн.

Оновлення офісних програм:

К = 800 + 8000 = 8800 грн.

Загальні затрати складуть:

К = 22769 грн.

3.2 Розрахунок експлуатаційних витрат

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

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на розробку та впровадження алгоритму захисту;

- витрати на ліцензію іншого ПЗ.

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою антивірусу та інших ПЗ займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА} = 200$ грн/год.

Час на резервне копіювання займе 0,5 год/тиждень:

$$С = ТС^* Ф = 200*0,5*50 = 5000 \text{ грн.}$$

Час на підтримку ОС і офісного пакету займе 0,5 год/тиждень, затрати:

$$С = ТС^* Ф = 200*0,5*50 = 5000 \text{ грн.}$$

Час на підтримку антивірусного захисту займе 0,5 год/тиждень, затрати:

$$С = ТС^* Ф = 200*0,5*50 = 5000 \text{ грн.}$$

Час на коригування алгоритму – 0,5 год/тиждень:

$$С = ТС^* Ф = 200*0,5*50 = 5000 \text{ грн.}$$

Значення загальних річних поточних витрат складає:

$$С = 5000 + 5000 + 5000 + 5000 = 20000 \text{ грн.}$$

3.3 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п = 4$ год.;
- час відновлення після поломки, $t_в$ (в годинах), $t_в = 4$ год.;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 4$ год.;

– заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), Z_0 = 30000 грн.;

– заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 25000 грн.;

– кількість обслуговуючого персоналу, N_0, N_0 = 1;

– число співробітників, N_c, N_c = 4;

– прибуток , O (грн. на рік), O = 2000000 грн.;

– вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 1000 грн;

– число зламаного обладнання, I, I = 2;

– число поломок на рік, n, n = 4.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.4:

$$П_п = \frac{\sum_{N_c} Z_c}{160} \cdot t_п, \text{ грн.}, \quad (3.4)$$

де місячний фонд робочого часу при 40-а годинному робочому тижні 160 годин.

Підставивши вихідні дані отримаємо:

$$П_П = (4*25000/160)*4 = 2500 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.5:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.6),

$П_{пв}$ – вартість відновлення обладнання (формула 3.7).

$$П_{ви} = \frac{\sum_{N_c} Z_c}{160} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ви} = (4*25000/160)*4 = 2500 \text{ грн.}$$

$$П_{пв} = (1*30000/160)*4 = 750 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 1000 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 2500 + 750 + 1000 = 4250 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.8 й 3.9 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.9)$$

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

$$V = (2000000/2080)*(4+4+4) = 11538,46 \text{ грн.}$$

$$U = 2500 + 4250 + 11538,46 = 18288,46 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.10):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.10)$$

$$ОУ = 4 * 2 * 18288,46 = 146307,68 \text{ грн.}$$

3.4 Загальний ефект від впровадження політики безпеки

Загальний ефект від впровадження алгоритму для компанії визначається за формулою 3.11 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн}, \quad (3.11)$$

де *ОУ*– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн.;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 146307{,}68 * 0{,}25 - 20000 = 16576{,}92 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.12 та терміну окупності капітальних інвестицій T_o за формулою 3.13.

$$ROSI = \frac{E}{K}, \text{ частки одиниці}, \quad (3.12)$$

де *E* – загальний ефект від впровадження системи захисту, грн.;

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

Підставивши відповідні значення, маємо:

$$\text{ROSI} = 16576{,}92 / 22769 = 0{,}73$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості.

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.13)$$

Підставимо значення:

$$T_o = 1 / 0{,}73 = 1{,}37 \text{ року (16 місяців).}$$

3.6 Висновки до третього розділу

У даному розділі була показана економічна доцільність впровадження запропонованої політики безпеки інформації інформаційно-комунікаційної системи, що доведено шляхом розрахунку:

- капітальних витрат на придбання та установку програмного забезпечення;
- експлуатаційних витрат на утримання та обслуговування програмного забезпечення;
- передбачуваних збитків від атак.

Розрахунки показали, що у випадку атаки на корпоративну мережу підприємства вартість збитків буде значно вищою, ніж вартість запропонованих засобів захисту. Термін окупності складає 1 рік і 4 місяці.

Таким чином, можемо зробити висновок, що запропонована система є економічно вигідною і рекомендується до впровадження на підприємстві.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було розглянуто та проаналізовано: найбільш актуальні загрози інформаційній безпеці для малих комерційних підприємств; розглянута узагальнена методика управління ризиками та система управління інцидентами інформаційної безпеки; розглянуті основні принципи, на яких повинна базуватися політика безпеки інформації на підприємстві; проведено аналіз нормативно-правової бази у сфері захисту інформації; виконана постановка задачі кваліфікаційної роботи.

В другому розділі було проведено обстеження об'єкта інформаційної діяльності; визначено і виконано категоріювання інформації, що циркулює в інформаційній системі; розроблено аналіз загроз та порушника; розроблено політику безпеки інформації для інформаційної системи.

В економічній частині розраховано витрати на розробку політики безпеки ТОВ «Аквамарин».

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України «Про основи національної безпеки України»;

2 ГСТУ СУІБ 1.0/ISO/IEC 27001:2010;

3 НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

4 НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп'ютерних системах від НСД (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

5 НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

6 НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53);

7 НД ТЗІ 2.5-005-99: 2012 60 автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);

8 НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22).;

9 НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (введено в дію Наказом ДСТСЗІ СБУ від 28.04.199 р. № 22) ;

10 Закон України «Про боротьбу з тероризмом»;

11 Закон України «Про інформацію»;

12 Закон України «Про захист інформації в автоматизованих системах»;

13 «Стратегія національної безпеки України»;

14 Навчальний посібник «Технології захисту інформації». Остапов Сергій Едуардович, Євсеєв Сергій Петрович, Король Ольга Григорівна.

15 Захист інформації. Навчальний посібник. Ч.1. (Організаційно-правові засоби забезпечення інформаційної безпеки) – 83 с.

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	2	
5	А4	Розділ 1	13	
6	А4	Розділ 2	57	
7	А4	Розділ 3	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії.

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

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-1 Глухих Р.О. на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Аквамарин»

Пояснювальна записка містить 94 сторінки, 5 рисунків, 15 таблиць, 4 додатки, 15 джерел.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки інформаційно-комунікаційної системи ТОВ «Аквамарин».

В ході виконання кваліфікаційної роботи було розглянуто та проаналізовано найбільш актуальні загрози інформаційній безпеці для малих комерційних підприємств; розглянута узагальнена методика управління ризиками та система управління інцидентами інформаційної безпеки; проведено аналіз нормативно-правової бази у сфері захисту інформації; виконана постановка задачі кваліфікаційної роботи.

В другому розділі було проведено обстеження об'єкта інформаційної діяльності; визначено і виконано категоріювання інформації, що циркулює в інформаційній системі; розроблено аналіз загроз та порушника; розроблено політику безпеки інформації для інформаційної системи.

В економічній частині розраховано витрати на розробку політики безпеки ТОВ «Аквамарин».

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

В якості недоліків слід відзначити окремі невідповідності вимогам при оформленні та недотримання термінів виконання.

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

В цілому робота задовольняє усім вимогам, а її автор Глухих Р.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**