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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Гапончука Антона Володимировича*

академічної групи *125–20–2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо–професійною програмою *Кібербезпека*

на тему ***Розробка політики безпеки інформації інформаційно–комунікаційної системи ТОВ ArchBuild.***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Магро В.І.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
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 ***Гапончуку А.В.*** **академічної групи** ***125–20–2***
(прізвище ім'я по–батькові) (шифр)

спеціальності ***125 Кібербезпека***
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно–комунікаційної системи ТОВ ArchBuild.***

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

Розділ	Зміст	Термін виконання
Розділ 1	Дослідити стан питання, проаналізувати нормативно–правову базу, постановка задач.	14.06.2024
Розділ 2	Провести обстеження будівлі та ІТС компанії, проаналізувати та класифікувати інформацію, створити модель порушника та модель загроз, обрати профіль захищеності, розробити елементи політики безпеки.	17.06.2024
Розділ 3	Розрахувати економічну доцільність витрат на впровадження політики безпеки.	20.06.2024

Завдання видано _____ Валерій МАГРО
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Антон ГАПОНЧУК
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 63 с., 11 рис., 6 табл., 6додатка, 18_джерел.

Предмет розробки: політика безпеки інформації інформаційно–комунікаційної системи ТОВ ArchBuild.

Об'єкт розробки: інформаційно–комунікаційна система ТОВ ArchBuild

Мета роботи: підвищення рівня захисту інформації в ІКС ТОВ ArchBuild шляхом розробки політики безпеки інформації.

У першому розділі описано стан питання, розглянуто нормативно–правову базу, проаналізовано стан забезпечення захисту інформаційної на малих підприємств та визначені види загроз. Було виконано постановку задачі.

У другому розділі було розглянуто ІКС обраної компанії. Обстежено об'єкт інформаційної діяльності, проаналізовано та класифіковано інформацію що зберігається та циркулює на підприємстві. Побудовано модель порушника та модель загроз. На підставі побудованих моделей було визначено актуальні проблеми у ІКС компанії та розроблено основні елементи політик безпеки.

У третьому розділі було розраховано витрати на впровадження політики безпеки, щорічні експлуатаційні витрати на її підтримку, доведено економічну доцільність впровадження розробленої політики безпеки.

Практична цінність розробки полягає у підвищенні рівня безпеки інформації у ІКС компанії ТОВ ArchBuild.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ABSTRACT

Explanatory note: 63 pp., 11 pic., 6 table, 6 app 18 sources.

The subject of development: the information security policy of the information and communication system of ArchBuild LLC.

Object of development: information and communication system ArchBuild LLC.

The purpose of the work: to increase the level of information protection in the ICS of ArchBuild LLC by developing an information security policy.

In the first section, the state of the issue is described, the regulatory and legal framework is considered, the state of information protection in small enterprises is analyzed and the types of threats are identified. The task statement was completed.

In the second section, ICS of the selected company was considered. The object of information activity was examined, the information stored and circulated at the enterprise was analyzed and classified. The offender model and the threat model were built. On the basis of the built models, actual problems in the company's ICS were identified and the main elements of security policies were developed.

In the third section, the costs of implementing the security policy were calculated, the annual operating costs for its support, and the economic feasibility of implementing the developed security policy was proved.

The practical value of the development lies in increasing the level of information security in the ICS of ArchBuild LLC.

SECURITY POLICY, THREAT MODEL, INTRUDER MODEL, INFORMATION SYSTEM, CYBERSECURITY, INFORMATION SECURITY MANAGEMENT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ЖК – житловий комплекс;

ЗП – заробітна плата;

ІКС – інформаційно–комунікаційна система;

ІзОД – інформація з обмеженим доступом;

КС – комп'ютерна система;

КЗЗ – комплекс засобів захисту;

ОС – операційна система;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ПБ – політика безпеки;

ТОВ – товари́ство з обме́женою відповіда́льністю;

DDoS – Distributed Denial of Service Attack;

IP – Internet Protocol;

SQL – Structured Query Language;

DNS – Domain Name System;

ЗМІСТ

с.

ВСТУП

З кожним роком кількість кібератак зростає, тим самим і зростає потреба у забезпеченні інформаційної безпеки, також зростає конкуренція між розробниками АС та ІКС адже кожен намагається створити свою систему найбільш легкою у реалізації та зручною. Об’єктом дослідження є інформаційно–комунікаційна система малого товариства, актуальність забезпечення безпеки ІКС малих підприємств зростає з кожним роком, за останні два роки кількість кібератак на малі підприємства зросла вдвічі, оскільки малі підприємства розглядаються зловмисниками як легкі цілі через їх обмежені ресурси.

Об'єктом розробки є політики безпеки інформації ІКС.

Предметом розробки є політика безпеки інформації інформаційно–комунікаційної системи.

Метою роботи є підвищення рівня захисту інформації в ІКС ТОВ ArchBuild шляхом розробки основних елементів політики безпеки інформації.

До задач кваліфікаційної роботи буде входити розробка основних елементів політики безпеки інформації інформаційно–комунікаційної системи, аналіз можливих загроз.

Практична цінність розробки полягає у підвищенні рівня безпеки інформації у ІКС компанії ТОВ ArchBuild.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Забезпечення захисту ІКС малих підприємств від кібератак стає з кожним роком все більш і більш актуальним. Кількість кібератак на малі та середні підприємства подвоїлась з весни 2022 року[1], атаки на малий бізнес становить 43% від всіх щорічних кібератак[2]. Таке велике зростання кіберзлочинності можна пояснити різними факторами на сам перед зростання кількості малих підприємств та значним стрибком у цифровізації.

У даний час цифровізація стала критично важливою складовою всіх підприємств від малих до світових корпорацій. Адже впровадження цифровізації допомагає підприємствам у всіх можливих сферах діяльності[5].

Цифровізація значно підвищує ефективність та продуктивність але з використанням автоматизації також і зростають ризики у кібербезпеці з'являються нові загрози такі як:

–фішингові атаки – кожен співробітник може стати ціллю що призведе до витоку інформації. Однак фішингові атаки лише початок який дає розуміння що компанія вже стала цілю та слід підвищити пильність;

–вразливості у ПЗ – використання застарілого ПЗ або неправильно налаштоване ПЗ може стати великою проблемою та значним пробілом у безпеці компанії що призведе до значних втрат;

Атаки на вебресурси компанії стають цілями зловмисники для DDoS–атак що завадить взаємодії з клієнтами та взагалі може паралізувати діяльність компанії, також до вебресурсів можуть використати SQL–ін'єкції що можуть дати зловмисникам знаний об'єм конфіденційних даних.

DDoS–атака – Distributed Denial of Service або розподілена атака типу "відмова у обслуговуванні" це тип кібератаки, мета якої – вивести з ладу або порушити роботу інтернет–сервісів, таких як вебсайти або мобільні програми та зробити їх недоступними для користувачів. DDoS–атаки зазвичай здійснюються шляхом переповнення сервера жертви більшою кількістю трафіку, ніж той може обробити.

За даними Cloudflare вже за перший квартал 2024 року лише системи Cloudflare змогли відбити 4.5 мільйона DDoS–атак, це на 50% більше ніж за минулий рік[6], графік показано на рис.1.

З кожним роком кількість та масивність атак зростає щорічно, це знано збільшує попит на якісні методи захисту від таких атак.

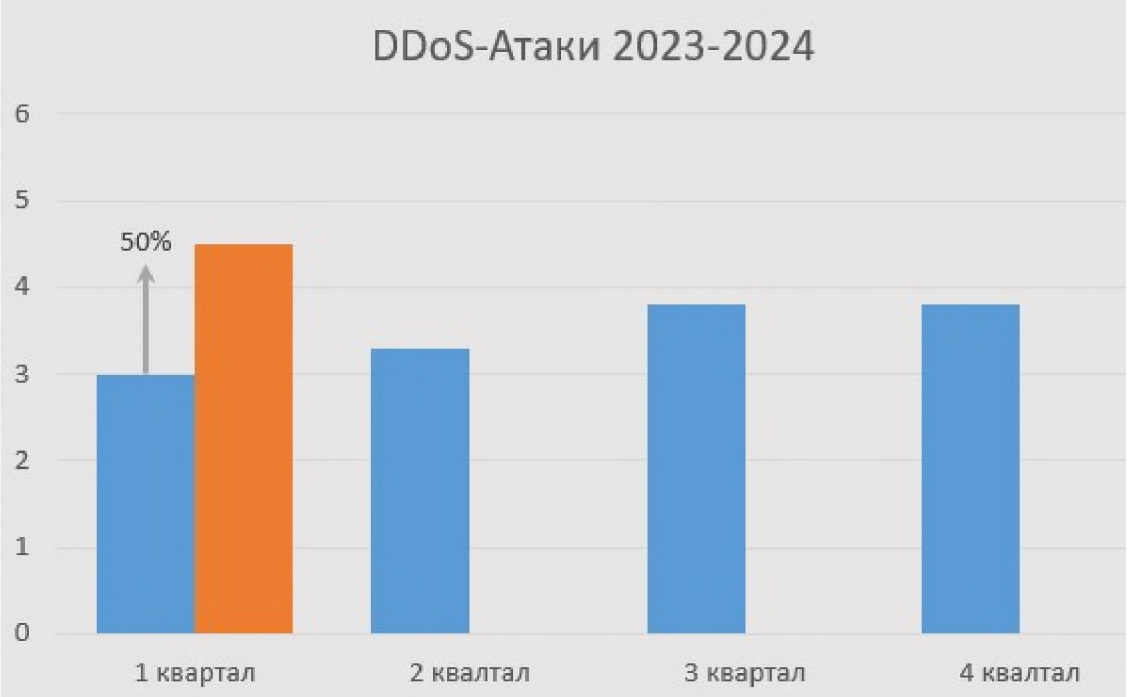

Рисунок 1.1 – Кількість DDoS–атак за квартали [6]

Кількість DDoS – атак на базі DNS збільшилась на 80% [6]наведено на рис.2 у порівнянні з минулим роком та залишаються найбільш популярною атакою.

NS – це протокол, який відповідає за перетворення доменних імен в IP адреси, що дозволяє користувачам отримувати доступ до вебсайтів та інших ресурсів в Інтернеті. Атака DNS–флуд – це, DDoS–атака, націлена на інфраструктуру DNS із використанням трафіку DNS–запитів і відповідей. Під час атаки DNS–флуд зловмисник переповнює DNS–сервери великою кількістю DNS–запитів або відповідей, спричиняючи їх сповільнення або збій. Це може призвести до простою вебсайту, низької швидкості Інтернету та інших збоїв. Атаки DNS–флуд можуть запускатися з мереж скомпрометованих пристроїв, таких як бот–нети, що ускладнює їх відстеження та зупинку.

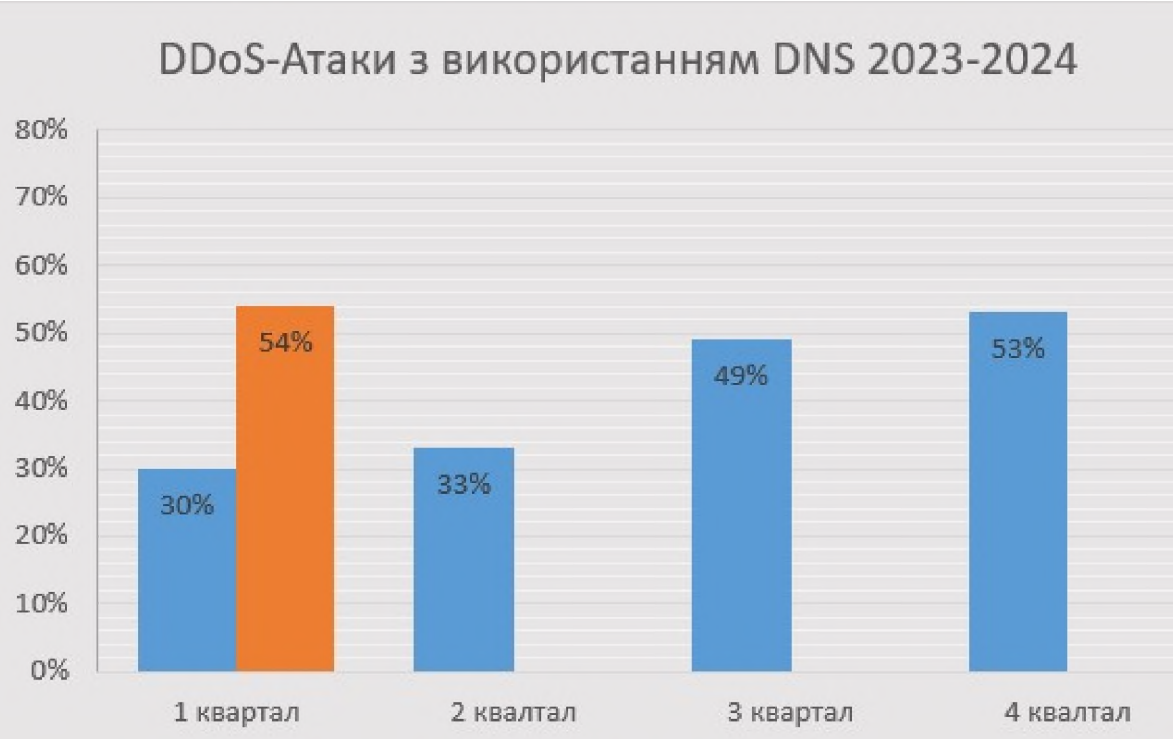

Рисунок 1.2 – Кількість DDoS–атак на основі DNS[6]

Також на графіку що зазначено на рис.2 можна побачити що у минулому році кількість атак на основі DNS тільки зростає з кожним кварталом при збереженні такої тенденції кількість компаній що будуть атаковані зростатиме, тому загрозу DDoS–атак не можна ігнорувати та вона все більш зростає.

DDoS–атаки на Швецію зросли на 466% після її прийняття до альянсу НАТО, що спостерігалось під час вступу Фінляндії до НАТО у 2023 році[6].

З кожним роком зростає індустрія ігор і азартних ігор які стали номером один, найбільшими підключеними HTTP–DDoS–атаками. Чуть більше половини з кожних 100 DDoS–запитів, які вдалося зм'якшити Cloudflare, були спрямовані на індустрію ігор і азартних ігор (рис.3 блакитний графік). На другому місці індустрія інформаційних технологій та Інтернету (помаранчевий графік), на третьому – маркетинг і реклама (сірий) . Далі індустрія ПЗ, криптовалюта та телекомунікації.

Кількість DDoS – атак на базі DNS збільшилась на 80% [6]наведено на рис.2 у порівнянні з минулим роком та залишаються найбільш популярною атакою.

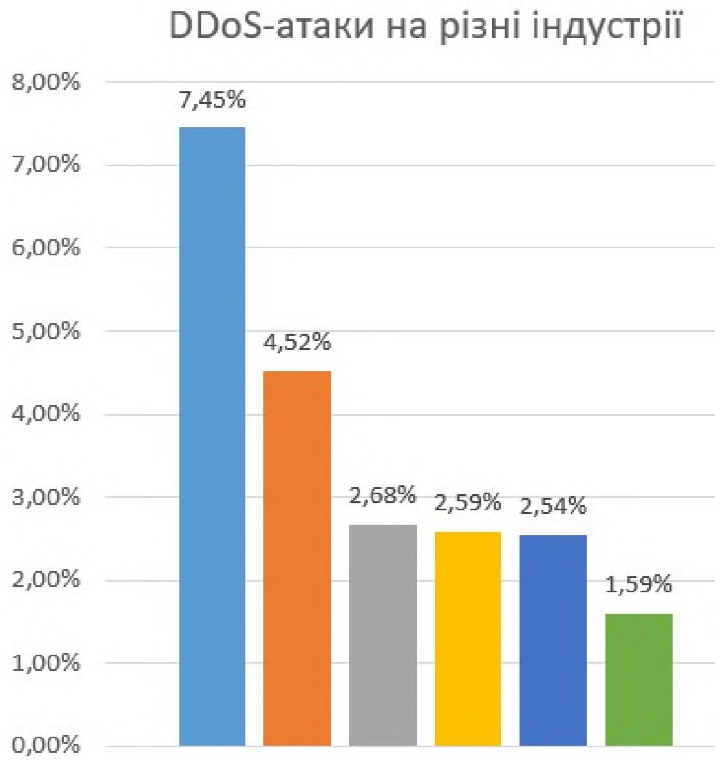

Рисунок 1.3 – DDoS – атак у різних сферах[6]

За перший квартал 2024 року США стала найбільшим джерелом HTTP–трафіку DDoS–атак, оскільки за статистикою Cloudflare (рис.4) 20% всіх запитів DDoS–атак була з IP–адресів США. Китай зайняв друге місце, далі Германія, Індонезія, Бразилія.

Рисунок 1.4 – Кількість DDoS–атак з різних країн. [6]

Також атаки на вебресурси компаній можуть бути з використанням SQL–ін'єкцій це атаки які використовують зловмисний код SQL для маніпулювання серверною базою даних для доступу до інформації, яка не призначена для відображення. Ця інформація може включати будь–яку кількість елементів, включаючи конфіденційні дані компанії, списки користувачів або приватні дані клієнтів.

SQL–ін'єкції можуть призвести не тільки до витоку конфіденційної інформації, а також і до того що зловмисник зможе модифікувати дані прямо у базі або взагалі видали. Зловмисники можуть використовувати SQL–ін'єкції для отримання доступу до системи з адміністративними привілеями, що дозволяє їм виконувати інші атаки або використовувати ресурси підприємства.

Також статистика показує що лише 14% малих підприємств що стали цілями були підготовленими до подібних атак[4]. Що показує зростання цифровізації про те дуже мала частина підготувалась до ризиків пов'язаних з переходим до цифровізації.

Через це середні збитки компаній від кібератак на малий та середній бізнес знаходиться у межах від 826 до 653 587 доларів США[4]. Така статистика дає побачити широкий вплив кіберзлочинності на бізнес.

За даними всесвітнього економічного форуму 95% інцидентів пов'язаних з кібербезпекою є людський фактором[4].

Малий бізнес що року стикається з серйозними проблемами у сфері кібербезпеки через обмежені ресурси та відсутність досвіду. Однак знецінення важливості кібербезпеки може призвести до катастрофічних наслідків.

Вже понад 87% підприємств маю та обробляють різні дані клієнтів[3] що можуть бути скомпрометовані у результаті різних кібератак що підкреслює важливість по забезпеченню кращого захисту від кібератак. Майже 40% малих підприємств повідомляють про втрати даних через кібератаки що призвело до значних втрат. За даними статистики[4] 75% підприємств малого та середнього бізнесу навіть не зможуть працювати якщо до їх системи потрапить програма вимагач, що може навіть призвести до закриття компанії.

Також важливим буде підкреслити що 80% інцидентів напряму пов'язані з компроментацією облікових даних та паролів[4]. Лише 17% мали підприємств шифрують дані що є важливою мірою у забезпеченні захисту конфіденційної інформації від несанкціонованого доступу, а 47% підприємств[4] загалі не мають окремого бюджету на кібербезпеку що є значним недоліком у забезпечені безпеки даних.

Компанія Cybersecurity Insiders провівши опитування серед різноманітних підприємств[10] з'ясувала що:

Лише 28% компаній відповіли, що використовують автоматизацію для моніторингу активності користувачів.

14% компаній взагалі не слідкують за активністю користувачів

28% компаній зазначили, що відстежують лише журнали допуску

17% компанії відстежують конкретні активності користувачів лише за певних обставин.

10% компаній відстежують активності користувачів лише після, певних інцидентів

Важливим фактором для забезпечення захисту інформації є аналіз можливих загроз. Ідентифікація, оцінка та пріоритезація потенційних загроз що можуть вплинути на безпеку даних, такі фактори є ключовими елементами які допомагають підприємствам впливати на вразливі місці та розробляти стратегії захисту.

Ідентифікація активів – визначення всіх активів що можуть стати цілю та зазначення важливості кожного активу для визначення який актив потребує найбільшого захисту.

Виявлення загроз – існують різні типи загроз внутрішні, зовнішні та природні. До внутрішніх загроз відносяться ненавмисні дії співробітників, інсайдерські атаки, використання вразливого ПЗ, помилки у налаштуваннях.
Зовнішні загрози це такі як фішингові атаки, DDoS–атаки, хакери, зловмисне ПЗ. До природних відносять різні природні катастрофи: пожежі, землетруси, повені, різні природні явища що можуть завдати збитків як незнаних так і достатньо вагомих.

Оцінка вразливостей – важлива складова що допомагає виявити недоліки у ПЗ, мережевій архітектурі та процесах управління.

Аналіз ризиків дозволе оцінити ймовірність того що конкретна вразливість буде використана, визначить ймовірні наслідки успішної атаки на компанію, включаючи фінансові втрати, втрату репутації, порушення працездатності.

Розробка стратегій захисту суттєво знизить ймовірність реалізації тих чи інших загроз, використання механізмів контролю таких як брандмауер, системи виявлень вторгнень, шифрування, політика доступу. Плани реагування допоможуть швидко та ефективно відновити систему та робочий процес після атаки. Також впровадження систем постійного моніторингу що дозволить відстежувати загрози та швидко на них реагувати.

Проведення тестування безпеки допоможе виявити які залишились вразливості та оцінити ефективність вже впроваджених заходів безпеки. Регулярні аудити та ревізії допоможуть дотриманню політики і процедур безпеки.

Також навчання персоналу підвищить обізнаність співробітників про загрози та методи захисту, проведення тренувань і симуляцій для підготування персоналу до можливих інцидентів.

Також треба постійно оновлювати систему та вдосконалювати методи захисту на основі нових загроз та вразливостей.

Аналіз загроз це безперервний процес оскільки загрози постійно вдосконалюються та постійно виникають нові вразливості, системний підхід до аналіз загроз дозволе компаніям бути готовою до різних типів загроз.

1.2 Аналіз нормативно–правової бази.

Розробка політики безпеки базується на багатьох нормативних документах та законах.

Закон України “Про інформацію” є одним з основних законодавчих актів, що регулюють сферу інформації в Україні. Цей закон визначає правові основи отримання, використання, поширення та зберігання інформації, а також регулює процеси здійснення цих прав і свобод.

НД ТЗІ 1.4–001–2000 цей нормативний документ регламентує діяльність служби захисту інформації у АС.

Закон України “про захист інформації в інформаційно–комунікаційних системах” встановлює правові основи для забезпечення захисту інформації, яка обробляється в інформаційно–комунікаційних системах. Він визначає основні принципи, завдання та засоби захисту інформації, регулює діяльність у цій сфері та встановлює відповідальність за порушення вимог захисту інформації.

НД ТЗІ 1.1–003–99 нормативний документ що зазначає терміни та визначення понять у галузі захисту інформації

НД ТЗІ 2.5–005–99 нормативний документ що слугує для класифікації АС та створення профілів захищеності інформації від несанкціонованого доступу.

НД ТЗІ 2.5–004–99 нормативний документ що встановлює критерії оцінки захищеності та є методологічною базою для визначення вимог захисту інформації.

НД ТЗІ 1.1–002–99 документ технічного захисту інформації слугує для вирішення завдань з захисту інформації та створення інших нормативних документів.

Закон України “про державну таємницю” регулює питання охорони державної таємниці, визначає її зміст, категорії, порядок засекречення та розсекречення інформації та встановлює відповідальність за порушення вимог цього закону.

Державна таємниця – це вид секретної інформації, що охоплює відомості в галузі оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці.

Існують різні рівні секретності інформації:

– особливої важливості;
– цілком таємна;
– таємна;

Цей закон є одним з ключових елементів системи національної безпеки України, спрямований на захист критичної інформації від загроз та забезпечення стабільності держави.

ДСТУ ISO/IEC 27001:2015 стандарт що визначає вимоги до проєктування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.

У результаті аналізу нормативно правової бази у галузі захисту інформації було виділено вимог, процедур та рекомендацій захисту інформації заснованих на вітчизняних та міжнародних стандартах, що є необхідним для забезпечення інформаційної безпеки.

1.3 Постановка задачі

З врахуванням актуальності проблем інформаційної безпеки на малих підприємствах, аналізу загроз та їх стрімкого щорічного зростання, слід забезпечити гарантований рівень інформаційної безпеки на підприємстві. Спеціальній частині необхідно проаналізувати особливості об'єкту інформаційної діяльності з точки зору забезпечення захисту інформації, виконати аналіз загроз створити модель порушника, обрати профіль захищеності, розробити основні елементи політики безпеки інформації.

1.4 Висновок

У першому розділі кваліфікаційної роботи було проаналізовано стрімкі темпи росту кібератак на малі підприємства, основні види внутрішніх та зовнішніх загроз. Проведено аналіз нормативно–правової бази, у результаті чого було виконано постановку задачі для спеціальної частини кваліфікаційної роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Основна інформація про вид діяльності ТОВ ArchBuild

ТОВ ArchBuild це невелика архітектурна компанія що розробляє власні проєкти, спеціалізується на сучасних рішеннях.

Компанія взаємодіє як з фізичними особами так і з юридичними, пропонуючи як власні вже готові проєкти так і отримує замовлення з побажаннями замовників.

Робочий графік компанії 5 днів на тиждень по 10 годин, з 09:00 до 19:00, обідня перерва з 13:00–13:30. Штат працівників складає 7 осіб, за необхідності компанія користується послугами найманого системного адміністратора, для оновлення ПЗ або вирішення інших проблем з ІКС чи ОС.

Розгорнутий штат працівників:

– керівник/головний архітектор, особа що відповідає за загальне керівництво компанією, приймає ключові рішення та контролює всі проєкти, координує роботу підрядників та контролює терміни і бюджет;

– архітектор–дизайнер, працює над створенням концептуальних дизайнів та архітектурних планів також спеціалізується на дизайні внутрішніх просторів та підборі матеріалів і меблів;

– інженер конструктор, забезпечує структурну цілісність будівельних проєктів, створює інженерні креслення;

– бухгалтер, веде фінансовий облік компанії, контролює витрати та доходи, складає фінансові звіти;

– юрист, забезпечує юридичну підтримку проєктів, готує договори та документи, консультує з юридичних питань;

– кресляр, працює над створенням детальних креслень та технічних документів для проєктів;

– адміністратор, організовує адміністративні процеси в офісі, веде документацію, забезпечує комунікацію між співробітниками та клієнтами;

2.2 Інформація що циркулює на об’єкті інформаційної діяльності.

У компанії циркулює інформація з обмеженим доступом, вся інформація зберігається у електронно, інформація зберігається у хмарному сховищі Google Drive.

Перелік інформації що обробляється на об’єкті інформаційної діяльності:

1.Персональні данні співробітників та клієнтів компанії, інформація з обмеженим доступом та віднесена до конфіденційної.

2.Фінансова інформація компанії, інформація з обмеженим доступом та віднесена до конфіденційної.

3.Адміністративна інформація, інформація з обмеженим доступом та віднесена до конфіденційної.

4.Інформація охоронної системи, інформація з обмеженим доступом та віднесена до конфіденційної.

5.Проєктна інформація, інформація з обмеженим доступом та віднесена до комерційної таємниці.

6.Інформація про замовлення, інформація з обмеженим доступом та віднесена до комерційної таємниці.

2.3 Обґрунтування необхідності створення КСЗІ

Виходячи з положенням законодавства України що до захисту інформації, було проведено категоріювання об’єкта та створено акт категоріювання (Додаток Е). За розпорядженням власника компанії було створено наказ про створення КСЗІ (Додаток Д) у якому було визначено необхідність створення КСЗІ та встановлено відповідальних осіб.

2.4 Організація роботи у компанії.

Компанія налічує 7 співробітників цикл робити описано нижче та зазначено на рис. 2.1

Адміністратор, організовує адміністративні процеси в офісі, веде документацію, забезпечує комунікацію між співробітниками та клієнтами. Першим зустрічає клієнтів та консультує їх з більшості питань, за потреби або якщо клієнт готовий укладати угоду, адміністратор спрямовує клієнта до керівника.

Керівник/головний архітектор, особа що відповідає за загальне керівництво компанією, приймає ключові рішення та контролює всі проєкти, координує роботу підрядників та контролює терміни і бюджет. Для укладання угоди між компанією на клієнтом керівник надає юристу завдання підготувати договір.

Юрист, забезпечує юридичну підтримку проєктів, готує договори та документи, консультує з юридичних питань.

Після укладання договору керівник надає вказання архітектору та інженеру, архітектор–дизайнер, працює над створенням концептуальних дизайнів та архітектурних планів також спеціалізується на дизайні внутрішніх просторів та підборі матеріалів і меблів.

Інженер конструктор, забезпечує структурну цілісність будівельних проєктів, створює інженерні креслення, після чого всі напрацьовані матеріали надаються кресляру який працює над створенням детальних креслень та технічних документів для проєктів. Який в свою чергу вже надає готовий проєкт та документацію до нього керівнику.

Рисунок 2.1 – Організаційна структура.

2.5 Обстеження об’єкту інформаційної діяльності.

Компанія розташована у жилій будівлі (ЖК Грані №2) рис.2.2 на першому поверсі, займає приміщення що з двох сторін півночі та заходу оточено зовнішніми стінами, зі сходу внутрішня стіна будівлі що відділяє приміщення компанії від кав’ярні, з південна стіна відділяє від службового приміщення керуючої компанії будівлі, у горі стеля межує з жилим приміщенням, а підлога з підземним паркінгом усі стіни та перекриття побудовані з залізобетону. Комунікації підведені через підвальні та службові приміщення управлінчої компанії.

Територія будинку не має огородженого зовнішнього периметра, з північного боку знаходиться пішохідний тротуар за ним дорога після якої розташовується паркова зона, з західного боку знаходиться велика територія з паркувальними місцями огороджена парканом доступ до якої здійснюється через проїзд зі шлагбаумом, поряд розташований ідентичний жилий будинок.

Рисунок 2.2 – Місце знаходження об’єкту інформаційної діяльності.

Вхід до приміщення компанії розміщено з північного боку будівлі, далі все відповідно до рис.2.3 Одразу на вході розміщено стійка адміністратору та його робоче місце, далі коридорне приміщення яке веде до інших кабінетів таких як праворуч від вхідного приміщення розміщується кабінет керівника, навпроти кабінету керівника розміщено спільний кабінет бухгалтеру та юриста, ліворуч від їх кабінету знаходиться спільний кабінет для інших співробітників та невелика зона відпочинку.

Рисунок 2.3 – Внутрішній план

Основні характеристики приміщень.

Компанія займає приміщення площею 84м2 див.рис.2.4, всі стіни виконані з залізо бетону, вхідні двері та вікна виходять на пішохідний тротуар та проїзджу частину за якою розміщується велика паркова зона. Вхідні двері замикаються на ключ як і всі двері що знаходяться у середині. Всі вікна (х2 вхідне приміщення та кабінет керівника) виконані з ПВХ пластику та є глухими вікнами(не мають механізму відкриття\закриття). Також на вхідних дверях та всіх вікнах розміщено залізні ролети що закриваються у неробочій час.

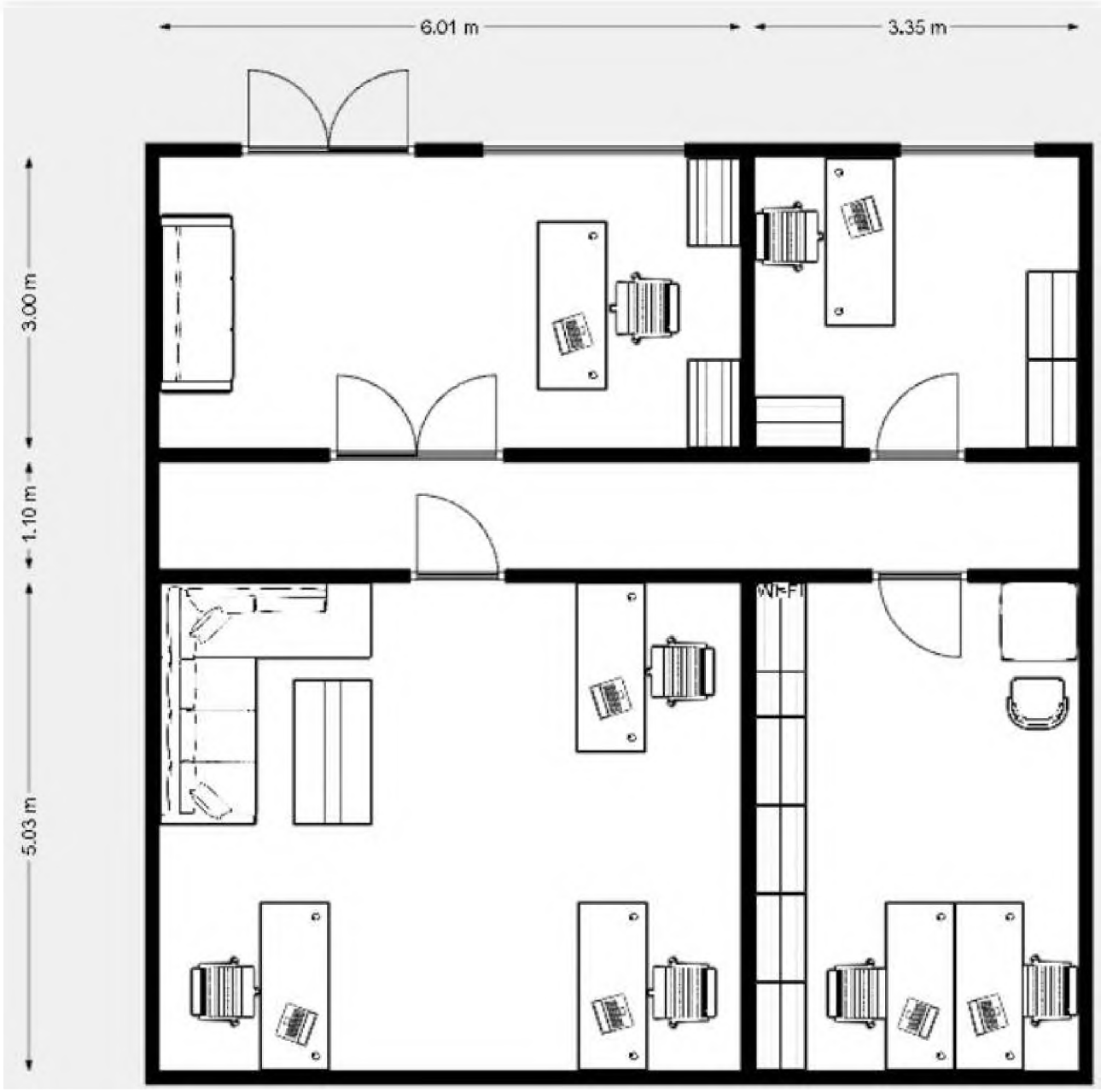

Рисунок 2.4 – Загальний план.

Всі потрібні комунікації прокладено через підвальні приміщення та пролягають вздовж стін та по стелі. Датчики диму розміщено у кожній кімнаті, два вогнегасники розміщено у двох кінцях коридору. Біля дверей вхідних дверей розміщено КПК охоронної системи що відповідає за забезпечення безпеки у неробочі години.

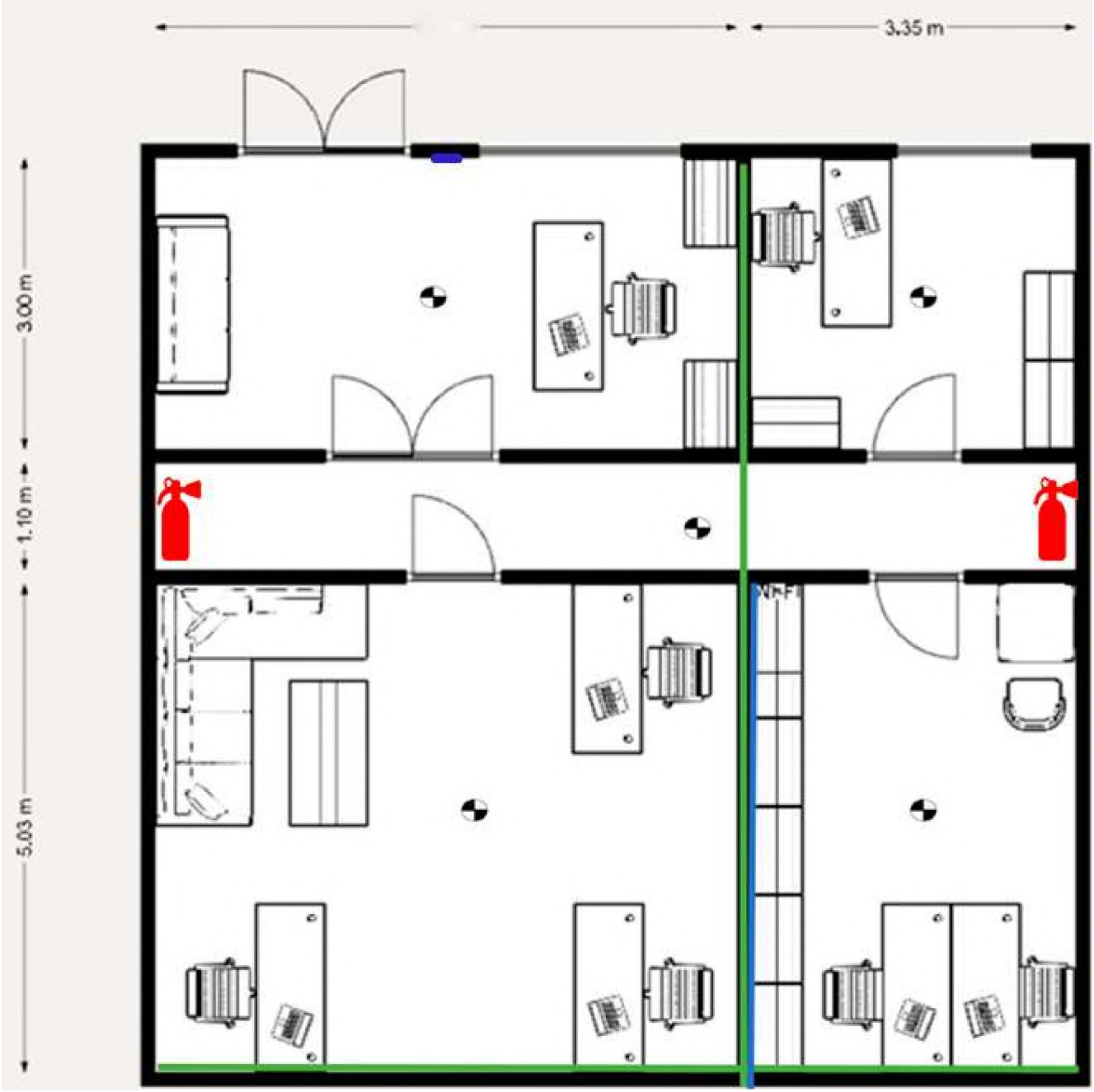

Рисунок 2.5 – Розміщення комунікацій.

2.6 Опис технічних засобів.

Компанія використовує не багато обладнання, а саме 1 Wi–Fi – роутер що розміщується на стіні у кабінеті бухгалтера і юриста та 7 ноутбуків що розміщені на кожному робочому місці.

Таблиця 2.1 – Технічне обладнання.

№	Назва	Марка	Модель	Серійний номер	Місце розміщення
1	Wi–Fi–роутер	AeroNet	ProMax 5000	BQ1234PO	Стіна у кабінеті бухгалтера і юриста
2	Ноутбук	Dell	XPS 17	RG4573K	Стіл у кабінеті керівника
3	Ноутбук	Dell	Inspiron 14 5000	TG7402KL	Стійка адміністратору
4	Ноутбук	Dell	Inspiron 14 5000	CV2054LK	Стіл бухгалтеру
5	Ноутбук	Dell	Inspiron 14 5000	VN0340QZ	Стіл юриста
6	Ноутбук	Dell	XPS 17	TY5930BC	Стіл архітектор–дизайнеру
7	Ноутбук	Dell	XPS 17	IE4920KS	Стіл інженера–конструктора
8	Ноутбук	Dell	XPS 17	AT5028GB	Стіл кресляра

У компанії використовують 7 ноутбуків про те не всі вони ідентичні так як різним співробітникам треба різне обладнання в залежності від їх діяльності.

До прикладу юристу чи адміністратору не треба пристрій з великими обчислювальними здібностями на відміну від дизайнеру чи інженеру.

Таблиця 2.2 – Технічні характеристики

№	Технічні характеристики	Найменування у мережі
1	Процесор:Intel Core i9,Опереративна пам'ять 32 Гб, Графіка NVIDIA GeForce RTX 3060, Накопичувачі SSD 2 Тб.	Ноутбук 1
2	Процесор:Intel Core i7,Опереративна память16 Гб, Вбудована графіка Intel Graphics, Накопичувачі HDD 1Тб, SSD 512 Гб.	Ноутбук 2
3	Процесор:Intel Core i7,Опереративна память16 Гб, Вбудована графіка Intel Graphics, Накопичувачі HDD 1Тб, SSD 512 Гб.	Ноутбук 3
4	Процесор:Intel Core i7,Опереративна память16 Гб, Вбудована графіка Intel Graphics, Накопичувачі HDD 1Тб, SSD 512 Гб.	Ноутбук 4
5	Процесор:Intel Core i9,Опереративна пам'ять 32 Гб, Графіка NVIDIA GeForce RTX 3060, Накопичувачі SSD 2 Тб.	Ноутбук 5
6	Процесор:Intel Core i9,Опереративна пам'ять 32 Гб, Графіка NVIDIA GeForce RTX 3060, Накопичувачі SSD 2 Тб.	Ноутбук 6
7	Процесор:Intel Core i9,Опереративна пам'ять 32 Гб, Графіка NVIDIA GeForce RTX 3060, Накопичувачі SSD 2 Тб.	Ноутбук 7

ПЗ що використовується на обладнані:

Операційна система Windows 10 Pro що встановлено на всіх ноутбуках компанії та придбано довічну ліцензію. Компанія використовує вбудований антивірус що не потребує придбання ліцензії. На всіх ноутбуках становлено

стандартній пакет ПЗ Microsoft Office 365 ліцензія придбано довічну разом з ОС. Також використовується безкоштовний браузер Google Chrome. На ноутбук бухгалтера встановлено спеціалізоване ПЗ QuickBooks, ПЗ для бухгалтерії та фінансового управління, ліцензію придбано на офіційному сайті. Також на ноутбуках 1,5,6,7 встановлено спеціалізоване ПЗ для створення проєктів, таке як: SketchUp Pro ПЗ для 3D–моделювання використовується для створення концептуальних задач, ліцензію придбано з щорічним оновленням. Autodesk AutoCAD Професійне ПЗ для креслення та проєктування, ліцензія придбано на офіційному сайті з щорічним оновленням.

2.7 Інформація у компанії

Вся інформація що оброблюється на підприємстві є з обмеженим доступом. Вона існує лише у цифровому форматі та зберігається у хмарному сховищі. Однак кожен вид інформації має свої вимоги до конфіденційності, цілісності та доступності.

Згідно до НД–ТЗІ–2.5–005–99, кожній циркулюючій інформації надано оцінку в умовних 1–3 одиницях де: 1 низькі вимоги, 2 середні, 3 високі, див.табл.2.3

Таблиця 2.3 Оцінка інформації

№	Вид інформації	конфіденційності	цілісності	доступності
1	Персональні данні співробітників та клієнтів	3	1	1
2	Фінансова інформація компанії	3	3	1
3	Адміністративна інформація	2	3	2
4	Інформація охоронної системи	3	1	1
5	Проєктна інформація	3	3	1
6	Інформація про замовлення	2	2	1

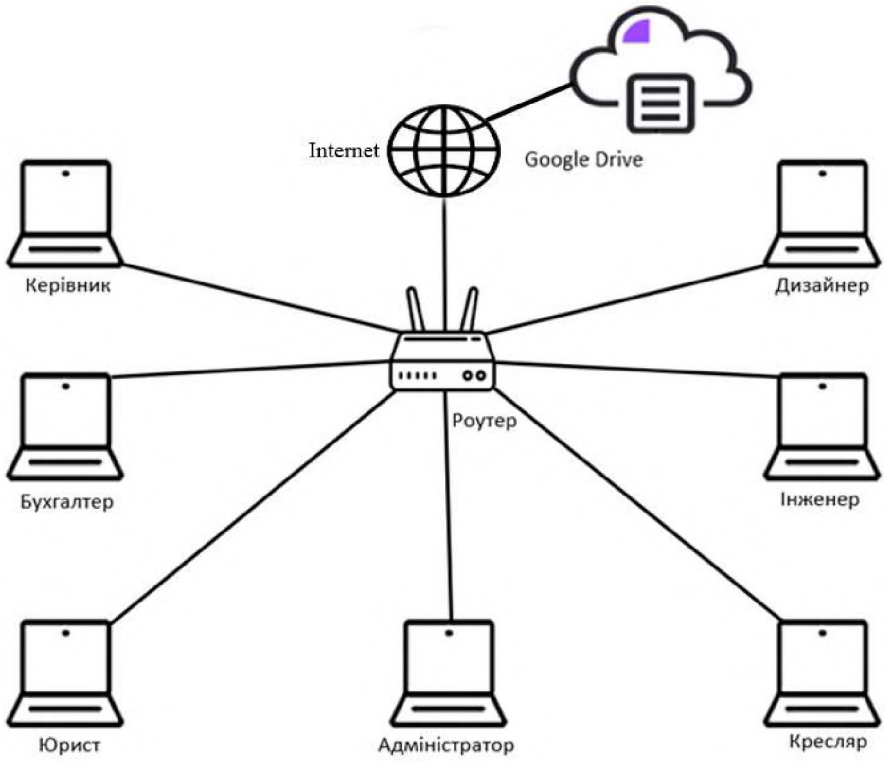

Рисунок 2.6 – Схема ІКС

В середині компанії циркулюють різні інформаційні потоки, а саме 1–робота з клієнтами, 2–розробка проєкту, 3–бухгалтерська,4–юридична, схема яких наведено нижче див. рис. 2.7

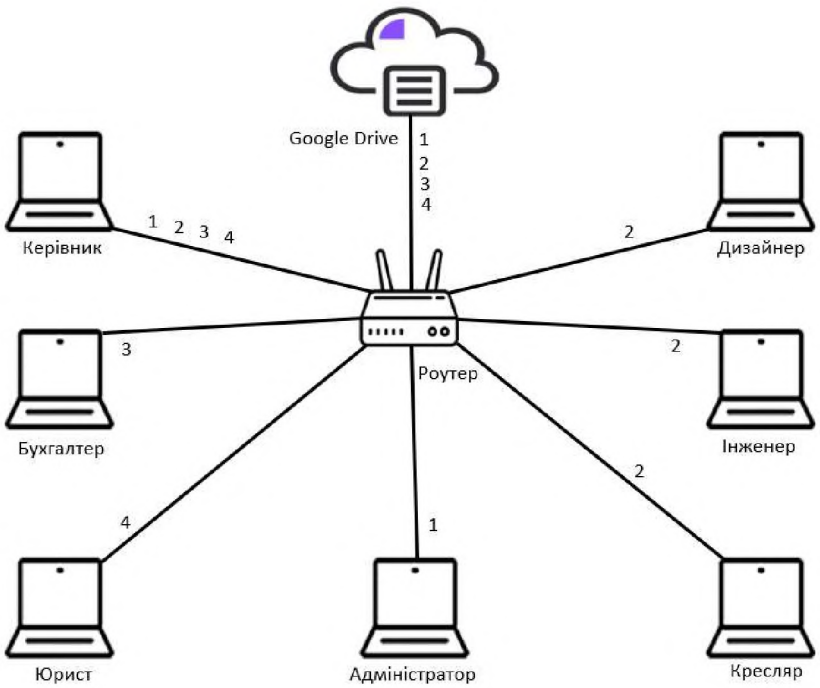

Рисунок 2.7 – Схема потоків інформації

2.8 Модель порушника

Порушником вважаються особи що мають намір отримати несанкціонований доступ до даних компанії, з різними цілями, метою порушника може бути:

–отримання необхідної інформації

–отримання можливості вносити зміни

–нанесення матеріальних збитків шляхом знищення інформації

Порушників зазвичай розділяють на два типи: внутрішній та зовнішній.

До внутрішніх порушників належать ті хто має фізичний доступ до ІТС, це може бути тимчасово найнятий персонал або співробітники компанії, той персонал що має безпосереднє відношення до ІТС.

До зовнішніх порушників належать ті особи що не мають право доступу до ІТС, до таких належать крадії, обслуговуючий персонал, конкуренти та інші.

Згідно до НД ТЗІ 1.4–001–2000 модель порушника слід складати за різними показниками:

–За метою порушника;

–За рівнем його можливостей;

–За рівнем знань АС;

–За їх методами;

–За місцем здійснення дій;

За сукупністю цих показників формується моделі можливих порушників.

Для оцінки загрози використано шкалу:

0 – не становить загрози

1 – низький рівень загрози

2 – середній рівень загрози

3 – високий рівень загрози

Спираючись на оцінку інформації (див.табл.2.3) що циркулює всередині компанії, конфіденційність має найвищий, цілісність має нижчий рівень, а доступність має низький рівень загрози.

Можливі мотиви:

А1 – Безвідповідальність

А2 – Самоствердження

А3 – Корисливий інтерес

Рівень можливостей:

Р1 – можливість підслуховувати чи підглядати

Р2 – використання недоліків та дозволених засобів

Р3 – використання технічних засобів

Рівень можливостей подолати систему захисту:

С1 – низький рівень

С2 – Має доступ и використання недоліків та дозволених засобів

С3 – Має високий рівень доступу чи використання технічних засобів

Рівень знань про систему:

З1 – має низький рівень знань про ІТС

З2 – має середній рівень знань про ІТС

З3 – має високий рівень знань про ІТС

Місце дій:

М1 – має доступ до приміщень але не до ІТС

М2 – має доступ до робочих місць

М3 – має повний доступ до ІТС

Таблиця 2.4 – Модель внутрішнього порушника.

Особа	Мотив	Можливість	Подолання захисту	Обізнаність	Місце	Сума загроз
Керівник	А2	Р3	С3	З3	М3	14
Адміністратор	А3	Р2	С1	З1	М2	9
Бухгалтер	А3	Р2	С1	З2	М3	12
Юрист	А3	Р2	С1	З2	М2	11
Інженер	А3	Р1	С1	З1	М2	8
Дизайнер	А3	Р1	С1	З1	М2	8
Кресляр	А3	Р1	С1	З1	М2	8
Найманий	А3	Р1	С1	З1	М2	8

Таблиця 2.5 – Модель зовнішнього порушника.

Особа	Мотив	Можливість	Подолання захисту	Обізнаність	Місце	Сума загроз
Колишні працівники	A3	P1	C1	З1	M1	7
Хакери	A3	P3	C3	З2	M3	14
Конкуренти	A3	P3	C2	З1	M1	10

Базуючись на даних таблиці 2.4 та таблиці 2.5, найбільшу небезпеку серед внутрішніх порушників становить директор оскільки він має найвищий рівень обізнаності системи та повний доступ до керування ІТС, володіє всією інформацією. Також до можливих внутрішніх порушників слід віднести бухгалтера та юриста, вони мають середній рівень обізнаності та можливостей.

Серед зовнішніх порушників найбільшу загрозу становить хакери, вони мають високий рівень кваліфікації та мають можливості до реалізації загроз навіть без доступу до ІТС. Також слід зауважити можливі загрози від конкурентів.

2.9 Модель загроз.

Після аналізу об’єкту кваліфікаційної роботи та ІТС згідно з НД ТЗІ 2.5–004–99 розглянуто перелік можливих загроз для конфіденційності, цілісності та доступності інформації компанії.

Таблиця 2.6. Загрози

Можливі загрози для інформації	Ризики для		
	К	Ц	Д
Можливі перебої у системі живлення	–	–	+
Відсутність доступу до інтернету	–	–	+
Несанкціоноване читання даних	+	–	–
Несанкціоноване підключення до мережі компанії	+	+	+
Несанкціоноване прослуховування	+	–	–
Розголошення паролів	+	+	+

Продовження таблиці 2.6

Пошкодження пристроїв	–	–	+
Модифікація ПЗ	–	+	+
Вхід до системи сторонніх осіб	+	+	+
Розголошення інформації персоналом	+	–	–
Ураження шкідливим ПЗ	+	+	+

2.10 Можливі вразливості інформаційно–комунікаційної системи.

У разі перебоїв у системі живлення, можливі проблеми з доступністю через відсутність безперебійного джерела живлення, також через скачки напруги підчас перебоїв можливий вихід з ладу робочих пристроїв.

У разі зникнення доступу до інтернету, обрив лінії, помилки провайдера та інше, через відсутність додаткової лінії інтернету буде втрачено доступність.

Через недосвідченість співробітників можливий перехід по сторонніх посиланнях у інтернеті, що може призвести втрати конфіденційності або до зараження шкідливим ПЗ.

Запуск стороннього ПЗ співробітниками що може призвести до зараження шкідливим ПЗ та втрати конфіденційності та цілісності.

У разі використання співробітниками зовнішніх носіїв інформації існує вірогідність зараження шкідливим ПЗ.

Також слід зауважити що найманий робітник може встановити стороннє ПЗ на пристрої що може призвести до втрати конфіденційності, цілісності, доступності.

2.11 Профіль захищеності.

Відповідно до НД–ТЗІ–2.5–005—99 що встановлює принцип класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Згідно з НД–ТЗІ–2.5–005—99 система компанії відноситься до класу 3 розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Відповідно до результатів аналізу загроз для підприємства було обрано наступний профіль захищеності:

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 }

Відповідно до НД–ТЗІ–2.5–005—99 КД–2 базова довірча конфіденційність. КЗЗ що має здійснювати розмежування доступу беручі за основу атрибути такі як:

–Процес та захищеність об’єкту;

–Користувача та захищеного об’єкту;

–Користувача, процесу та захищеного об’єкту;

У випадку з КД–2 використовується атрибут користувача та захищеного об’єкту. Запити на зміни прав доступу повинні опрацьовуватись КЗЗ на підставі атрибутів доступу користувача, КЗЗ повинен надати можливість користувачу визначити (у випадку КД–2) конкретних користувачів чи групу користувачів у яких є допуск отримувати інформацію від об’єкту. КЗЗ має надати можливість користувачеві визначити певних користувачів або групу користувачів що мають допуск запускати процеси. Права доступу до захищеного об'єкта мають бути встановлені у момент його створення або ініціалізації.

Згідно з НД–ТЗІ–2.5–005—99 для КД–2 базової довірчої конфіденційності треба НИ–1 зовнішня ідентифікація та автентифікація.

Політика ідентифікації і автентифікації, що реалізується КЗЗ, має бути визначена атрибутами, якими характеризується користувач та послугами, що потребують використання цих атрибутів. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити користувачу виконувати будь–які інші, контрольовані КЗЗ дії, КЗЗ повинен (у випадку НИ–1) з використанням захищеного механізму отримати від зовнішнього джерела автентифікований ідентифікатор цього користувача.

КО–1 повторне використання об'єктів відповідно до НД–ТЗІ–2.5–005–99 та обраним профілем захищеності КЦД.1. КО–1 є невід’ємним критерієм конфіденційності що належить обраному профілю.

КО–1 повторне використання об'єктів послуга що дозволяє забезпечити коректність повторного використання розділених об'єктів, гарантуючи, що в разі, якщо розділений об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

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. Це одна з послуг що забезпечує конфіденційність. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги залежать від повноти захисту і вибірковості керування.

Обравши КЦД.1 потребується КВ–1 мінімальна конфіденційність при обміні політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів та їх процесів, до яких вона відноситься.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься на об'єкті що розглядається.

Довірча цілісність послуга дозволяє користувачеві керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги варіюються на підставі повноти захисту та вибірковості керування. До обраного профілю захищеності належить ЦД–1 мінімальна довірча цілісність. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати

множину об'єктів КС, до яких вона відноситься, КЗЗ має здійснювати розмежування доступу на підставі обраних атрибутів доступу, (у випадку КЦД.1 = ЦД–1) обраний атрибут: користувача і захищеного об'єкта.

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

Для ЦД–1 мінімальна довірча цілісність є необхідна умова НИ–1, зовнішня ідентифікація і автентифікація, перш ніж дозволити будь–якому користувачу виконувати будь–які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від зовнішнього джерела автентифікований ідентифікатор цього користувача.

ЦО–1 обмежений відкат. Відкат послуга забезпечує можливість відмінити операцію або послідовність операцій та повернути захищений об'єкт до попереднього стану. Рівні даної послуги варіюються на підставі множини операцій, для яких забезпечується відкат.

ЦО–1 має необхідні умови для реалізації, а саме НИ–1 що вже виконано у попередніх рівнях.

ЦО–1 обмежений відкат політика відкату, що реалізується КЗЗ, 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 операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ–1 мінімальна цілісність при обміні, послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

ЦВ–1 мінімальна цілісність при обміні політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС та процесів, до яких вона належить, рівень захищеності, що забезпечується використовуваними механізмами та спроможність користувачів або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті.

ЦВ–1 Мінімальна цілісність при обміні не має необхідних умов для виконання.

ДР–1 послуга використання ресурсів дозволяє користувачам керувати використанням послуг і ресурсів.

ДР–1 квоти політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Політика використання ресурсів має бути визначеною обмеженням, що можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Необхідні умови для виконання ДР–1 це НО–1.

НО–1 виділення адміністратора або розподіл обов'язків послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.

НО–1 Виділення адміністратора політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

За для виконання умови НО–1 є необхідна умова НИ–1 що вже була виконана та описана вище.

Відповідно до профілю захищеності наступний необхідний атрибут це: ДВ–1

Відновлення після збоїв послуга що забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування.

ДВ–1 ручне відновлення політика відновлення, що реалізується КЗЗ, повинна визначати типи відмов КС та 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 КС відповідно до ДВ–1 обрано:

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС 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 КС до нормального функціонування.

Необхідні умови для ДВ–1, НО–1 послуга що вже була виконана то описана. Далі відповідно до обраного профілю захищеності йде критерій спостереження а саме реєстрація – дозволяє контролювати небезпечні для КС дії.

Згідно з обраним профілем необхідна послуга 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 та успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу 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.

Необхідні умови для реалізації послуги НР–2, не послуги НИ–1 та НО–1, послуги що були реалізовані раніше до попередніх послуг.

Згідно з обраним профілем захищеності слід реалізувати послугу 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 (відповідно до послуги НИ–2) автентифікувати цього користувача з використанням захищеного механізму.

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

За для реалізації послуги НИ–2 встановлено необхідні умови такі як реалізація послуги НК–1.

НК–1 одно–направлений достовірний канал послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем та КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватись виключно користувачем.

НО–2 розподіл обов'язків адміністраторів послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.

НО–2 розподіл обов'язків адміністраторів політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача та 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 ті 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.

Реалізація послуги НО–2 потребує реалізації послуги НИ–1, ця послуга вже була описана раніше.

НЦ–2 КЗЗ з гарантованою цілісністю я послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

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 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.

Реалізація послуги НЦ–2 не потребує додаткових умов для реалізації послуги.

НТ–2 само–тестування при старті дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. НТ–2 само–тестування при старті політика само–тестування, що реалізується КЗЗ, повинна описувати властивості КС та реалізовані процедури, що 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.

НТ–2 потребує для реалізації додаткові умови НО–1.

НВ–1 автентифікація вузла дозволяє одному КЗЗ ідентифікувати інший КЗЗ встановлювати та перевіряти його ідентичність і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.

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.

НВ–1 не потребує додаткових умов для реалізації.

2.12 Розробка політики безпеки.

Базуючись на результатах аналізу моделей загроз та порушників та спираючись на обраний профіль захищеності розроблено елементи політики безпеки для обраної компанії, що допоможуть знизити ризики з найбільшими рівнями загроз.

До таких загроз належать:

– читання інформації з екранів співробітників;

– ураження шкідливим ПЗ;

–використання соціальної інженерії;

2.12.1 Політика обізнаності про соціальну інженерію.

Мета:

Метою політики є інформування співробітників про можливі шахрайські атаки соціальної інженерії та методи якими співробітники можуть використати для виявлення атак.

Сфера застосування:

Ця політика розповсюджується на всіх працівників компанії.

Політика:

Конфіденційна інформація не буде передана сторонній особі якщо вона використовую такі фрази чи методи:

– “невідкладна справа”;

– “забутий пароль”;

– “надзвичайна ситуація”;

– будь які форми залякування з боку вищого керівництва;

– будь–яке «скидання імені» особою, яке створює видимість того, що воно походить від законного та уповноваженого персоналу;

– запитувач вимагає надати інформацію, яка розкриє паролі, модель, серійний номер, бренд або кількість ресурсів компанії;

Дії:

– усі співробітник мають пройти навчання з питань безпеки;

– при виявлені підозрілої особи “запитувача”, особа має бути перевірена перш ніж продовжити розмову або листування;

Відповідальність:

Працівник, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, аж до звільнення з роботи.

2.12.2 Політика захисту паролем

Мета:

Метою політики встановлення стандарту використання та захисту паролів.

Сфера застосування:

Ця політика розповсюджується на всіх співробітників та всі пристрої компанії.

Політика:

–всі співробітники мають використовувати різні унікальні паролі для своїх облікових записів;

–за можливості слід використовувати багатофакторну автентифікацію;

–співробітники можуть використовувати авторизовані, затверджені менеджери паролів;

–паролі слід змінювати лише тоді, коли є підстави вважати, що пароль було скомпрометовано або він не відповідає нашим вимогам до створення пароля;

–паролі не можна нікому повідомляти, навіть керівництву;

–паролі можуть зберігатися тільки в менеджерах паролів, авторизованих організацією;

Відповідальність:

Працівник, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, аж до звільнення з роботи.

2.12.3 Політика контролю програмного забезпечення.

Мета:

Метою цієї політики є регламентування що до інсталяції програмного забезпечення на пристрої компанії.

Сфера застосування:

Ця політика розповсюджується на всіх співробітників та всі пристрої компанії.

Політика:

–співробітники не мають права встановлювати програмне забезпечення на пристрої компанії;

–у разі потреби нового ПЗ, співробітнику слід дати запит на завантаження нового ПЗ, перш ніж встановити ПЗ запит має схвалити керівник компанії;

Відповідальність:

Працівник, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, аж до звільнення з роботи.

2.13.4 Політика резервного копіювання.

Мета:

Метою політики є встановлення порядку резервного копіювання щоб мати змогу відновити працездатність системи або інформації при втраті.

Сфера застосування

Ця політика розповсюджується на всіх співробітників та поширюється на всі пристрої компанії.

Політика:

–регулярно має відбуватись резервне копіювання;

–процес копіювання має бути задокументований;

–необхідно здійснювати підтвердження успішного копіювання;

–процес відновлення втрачених даних слід документувати;

–резервні копії системи мають зберігатись окремо від іншої інформації;

–резервне копіювання слід виконувати за протоколом 3–2–1, відповідно до якого треба створити три копії інформації, на двох різних носіях, а третя копія моє зберігатись у хмарному сховищі;

Відповідальність

Працівник, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, аж до звільнення з роботи.

2.13.5 Політика антивірусного захисту.

Мета:

Метою політики є зниження ризиків зараження ІТС вірусними програмними засобами.

Сфера застосування

Ця політика розповсюджується на всіх працівників компанії.

Політика:

–на кожному пристрої компанії має бути встановлено антивірусні засоби.

–антивірусне програмне забезпечення має бети завжди вчасно оновлено.

–у разі зараження шкідливим ПЗ пристрою, слід вилучити пристрій з мережі провести сканування та повне очищення від шкідливого ПЗ.

Необхідно ввести наступні вимоги для запобігання зараженню вірусним ПЗ:

–заборонено відкривати файли з електронних листів від ненадійних джерел.

–регулярно видаляти зайві електронні листи та чистити спам.

–заборонено завантажувати будь які файли з невідомих джерел.

–регулярне резервне копіювання важливих файлів та налаштувань.

Відповідальність

Працівник, що порушив цю політику, може бути притягнутий до дисциплінарної відповідальності, аж до звільнення з роботи.

2.14 Висновок

У другому розділі розглянуто ІКС обраної компанії. Обстежено об’єкт інформаційної діяльності, проаналізовано та класифіковано інформацію що зберігається та циркулює на об’єкті інформаційної діяльності. Побудовано модель порушника та модель загроз. На підставі побудованих моделей було визначено актуальні проблеми у ІКС компанії та розроблено основні елементи політики безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічне обґрунтування доцільності витрат на реалізацію політики безпеки.

Метою розрахунків є економічне обґрунтування витрат на впровадження політики безпеки інформації. Для цього треба провести розрахунки для визначення економічної ефективності використання основних результатів що тримані у ході виконання роботи.

Економічна доцільність визначається розрахунками:

– капітальних витрат, що потребує розроблена політика безпеки;

– експлуатаційних витрат;

– річного економічного ефекту від впровадження політики безпеки;

Капітальні витрати

Окремі запропоновані елементи політики безпеки потребують витрат на реалізацію, до таких відносяться:

–політика чистого столу

–політика антивірусного ПЗ

3.2 Розрахунок капітальних витрат

3.2.1Трудомісткість створення політики безпеки розраховується за формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \quad (3.1)$$

$t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, склало 6 години;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації, склало 9 години;

$t_{а}$ – тривалість процесу аналізу ризиків, склало 4 години;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, склало 5 годин ;

tозб – тривалість вибору основних рішень з забезпечення безпеки інформації, склало 8 годин;

tовр– тривалість організації виконання відновлювальних робіт ізабезпечення неперервного функціонування організації, склало 6 годин;

tд – тривалість документального оформлення політики безпеки, склало 3 години.

$$T = 6+9+4+5+8+6+3$$

$$t = 41 \text{ годину}$$

3.2.2 Розрахунок витрат на створення ПБ.

Витрати на розробку ПБ являються сумою витрат на заробітну плату спеціаліста і вартості витрат машинного часу, необхідного для розробки ПБ.

Та розраховуються за формулою:

$$Крп = Ззп + Змч \quad (3.2)$$

Крп – витрати на розробку політики безпеки інформації;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, необхідного для розробки ПБ;

Заробітна плата виконавця враховує основну, додаткову ЗП та соціальні відрахування та розраховується за формулою:

$$Ззп = t \cdot Зіб \text{ , грн} \quad (3.3)$$

t – загальна тривалість створення ПЗ, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$Ззп = 41 \cdot 200$$

$$Ззп = 8200 \text{ грн}$$

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

$$З_{мч} = t \cdot С_{мч}\ ,\ грн \qquad (3.4)$$

t – трудомісткість розробки політики безпеки інформації на ПК,годин;

Смч – вартість 1 години машинного часу ноутбуку, грн./годин

Вартість 1 години машинного часу ноутбуків визначається за формулою:

$$Смч = Р \cdot Се + \frac{Фзал \cdot На}{Fp} + \frac{Клпз \cdot Напз}{Fp} \qquad (3.5)$$

Р – встановлена потужність ноутбуку, кВт (0,4 кВт)

Се– тариф на електричну енергію, грн/кВт·година(1,68грн/кВт·година);

Фзал – залишкова вартість ПК на поточний рік, грн(Фзал = 9000 грн).;

На – річна норма амортизації на ПК, частки одиниці (1/3 на рік);

Напз – річна норма амортизації на ліцензійне програмне забезпечення,частки одиниці (100% на рік);

Клпз – вартість ліцензійного програмного забезпечення, грн (35500 грн);

Fp – річний фонд робочого часу (за 40–годинного робочого тижня Fp = 1920.)

$$Смч = 0{,}4 \cdot 1{,}68 + \frac{9000 \cdot 1/3}{1920} + \frac{35500 \cdot 1}{1920}$$

$$Смч = 0{,}672 + \frac{3000}{1920} + \frac{1775}{96}$$

$$Смч = \frac{84}{125} + \frac{25}{16} + \frac{1775}{96}$$

$$Смч = 20{,}72$$

$$Змч = 41 \cdot 20{,}72$$

$$Змч \approx 849{,}52$$

Крп =8200+850

Крп= 9050

Таким чином капітальні витрати на проєктування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Кпз + Кнавч + Кн, \text{ грн} \quad (3.6)$$

Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, а саме спеціаліст з розробки політики безпеки (Крп=8200)

Кзпз –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), а саме (основне ліцензія QuickBooks та SketchUp Pro) та додаткове(ліцензія антивірусу) (Кзпз=35500);

Крп – вартість розробки політики безпеки інформації, (Крп=9050);

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу. Для малого підприємства навчання дорівнює 500 грн за одного фахівця;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. не враховується так як підприємство не закуповує обладнання.

К = 8200+35500+9050+500=53250 грн

3.3 Розрахунок поточних витрат.

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

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ тис. грн.} \quad (3.7)$$

Св – вартість Upgrade–відновлення й модернізації системи ;

Ск – витрати на керування системою в цілому ;

Сак – витрати, викликані активністю користувачі системи інформаційної безпеки.

Витрати на керування системою в цілому ($С_к$) вираховується заформулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.8)$$

$С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н = 0$).

$С_а$ – річний фонд амортизаційних відрахувань вираховуються заформулою:

$$С_а = К_{зпз} * А \quad (3.9)$$

Єдине на що треба робити амортизаційні відрахування, на придбання ліцензійного програмного забезпечення, через це отримаємо, щорічний відсоток амортизації на 2 роки використання буде:

$$А = \frac{100}{2} \% = 50\%$$

$$К_{зпз} = 35500 \text{ грн}$$

Використовуємо формулу 3.9 та отримуємо:

$$С_а = 35500 \cdot 50\% = 17750 \text{ грн}$$

Сз – Річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.10)$$

$З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

$З_{осн}$ = 13 276 грн на місяць

$З_{дод}$ вираховується в розмірі 8–10% від основної заробітної плати.

$$С_з = 13276 \cdot 12 + (13276 \cdot 12 \cdot 0{,}08)$$

$$С_з = 159312 + 12744$$

$$С_з = 172056 \text{ грн на рік}$$

Для платників податків на спрощений системі ставка ЄСВ становить 22%, отже:

$$С_{єв} = 307243 \cdot 0,22$$

$$С_{єв} = 67593$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн.} \qquad (3.11)$$

Р – встановлена потужність апаратури інформаційної безпеки, кВт(Р= 1,5);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки($F_р$ = 1920);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин ($Ц_е$ = 1,68 грн/кВт·год)

$$С_{ел} = 1,5 \cdot 1920 \cdot 1,68 = 4838 \text{ грн}$$

Со – витрати на залучення сторонніх організацій, чого не відбувається.

$С_{тос}$ – витрати на технічне та організаційне адміністрування й сервіс системи інформаційної безпеки що визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає 1% від суми капітальних інвестицій що = 532 грн.

$$С_к = 0 + 17750 + 172056 + 67593 + 4838 + 532 = 262769$$

$$С = 0 + 262769 + 1000 = 263769 \text{ грн.}$$

3.4 Оцінка величини збитків.

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідокатаки, годин($t_п$ = 8);

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну

мережу, годин ($t_в = 3$);

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин($t_{ви} = 3$);

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів таін.), грн на місяць($З_о = 24000$);

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць($З_с = 26000$);

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.),осіб.($Ч_о = 1$);

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб. ($Ч_с = 7$);

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік (О = 3400000);

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн ($П_{зч}$ =5555);

I – число атакованих вузлів або сегментів корпоративної мережі(I = 7);

N – середнє число атак на рік (N = 5).

Розміри ЗП працівників компанії:

– керівник – 30000

– адміністратор – 25000

– бухгалтер – 27000

– юрист – 26000

– інші – 23000 * 3 = 69000

Сума = 177000

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \qquad (3.12)$$

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

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн;

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

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

$$П_п = \frac{\sum Зс}{F} \cdot t_п \quad (3.13)$$

F– місячний фонд робочого часу (при 50–а годинному робочому тижні становить 250 ч)

Пп = (177000/250)*8 = 5664

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

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.14)$$

$П_{ви}$ – витрати на повторне уведення інформації, грн;

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

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

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

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \quad (3.15)$$

Пви = (177000/250) * 3

$$Пви = 2124$$

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються часом відновлення після атаки і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв}= \frac{\sum Зо}{F} \cdot t_в \quad (3.16)$$

$$П_{пв}= (24000/250) \cdot 3$$

$$П_{пв} = 288$$

Далі по формулі (3.14):

$$П_в = 5664+2124+288$$

$$П_в = 8076$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо годинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V= \frac{О}{Fг} \cdot (t_п + t_в + t_{ви}) \quad (3.17)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5–ти денний робочий тиждень, 10–и годинний робочий день) становить близько 2600 ч.

$$V= \frac{3400000}{2600} \cdot (8+3+3)$$

$$V= 18846$$

Далі по формулі (3.12):

$$U = 5662 + 8076 + 18846 = 32584$$

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

$$B=\sum_i\sum_n U \quad (3.18)$$

$$B = 5 \cdot 7 \cdot 32584 = 1140440$$

3.5 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \quad (3.19)$$

$$E= 1140440 \cdot 0{,}5 - 263769$$

$$E=306451$$

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

$$ROSI = \frac{E}{K}$$

$$ROSI = \frac{306451}{53250}$$

$$ROSI = 5{,}75$$

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

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

$$5{,}75> ((13-5)/100)$$

$$5{,}75> 0{,}08$$

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

$$T_0 = \frac{K}{E} = \frac{1}{ROSI}, \text{ років}$$

$$T_0 = \frac{1}{5,75}$$

$$T_0 = 0,17 \text{ роки}$$

3.6 Висновок

У розділі проведено детальний аналіз витрат на впровадження та експлуатацію захисних систем, що включає як капітальні, так і експлуатаційні витрати. Встановлено, що інвестиції в інформаційну безпеку є економічно обґрунтованими, так як це значно зменшить ризики втрат від потенційних кібератак. Витрати на впровадження політики безпеки становлять 53250 грн, експлуатаційні витрати становлять 263769грн. Загальні збитки від атак складають 1140440грн, ефект від впровадження політики безпеки складає 306451грн, термін окупності інвестицій приблизно два місяці. За отриманими результатами впровадження політики безпеки є доцільним.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було описано стан інформаційної захищеності серед малих компаній, проаналізовано нормативно–правову базу документів сфери захисту інформації. Розглянуто основну проблему та потребу у впровадження політики безпеки для малих підприємств.

У другому розділі кваліфікаційної роботи обстежено об’єкт інформаційної діяльності, проаналізовано та класифіковано інформацію що зберігається та циркулює на об’єкті інформаційної діяльності. Побудовано модель порушника та модель загроз. На підставі побудованих моделей було визначено актуальні проблеми у ІТС компанії та розроблено основні елементи політики безпеки.

У третьому розділі кваліфікаційної роботи було проведено детальний аналіз витрат на впровадження та експлуатацію захисних систем, що включає як капітальні, так і експлуатаційні витрати. Встановлено, що інвестиції в інформаційну безпеку є економічно обґрунтованими, так як це значно зменшить ризики втрат від потенційних кібератак. Витрати на впровадження політики безпеки становлять 53250 грн, експлуатаційні витрати становлять 263769грн. Загальні збитки від атак складають 1140440грн, ефект від впровадження політики безпеки складає 306451грн, термін окупності інвестицій приблизно два місяці. За отриманими результатами впровадження політики безпеки є доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1. Щорічний звіт компанії Truesec про загрози та інформація про зміни загроз https://newsroom.truesec.com/posts/pressreleases/cyber–attacks–continue–to–increase–in–2024 (дата звернення 14.06.2024)

2. Статистика кібератак на малий бізнес https://www.getastra.com/blog/security–audit/small–business–cyber–attack–statistics/ (дата звернення 14.06.2024)

3. Інформація про кібератаки на малий бізнес https://www.stationx.net/cyber–attacks–on–small–businesses–statistics/ (дата звернення 14.06.2024)

4. Статистичні данні про кібератаки на малий бізнес https://smallbiztrends.com/small–business–cybersecurity/ (дата звернення 15.06.2024)

5. Про важливість впровадження інформаційних технологій у малий бізнес https://www.weforum.org/agenda/2023/07/digital–transformation–potential–smes/ (дата звернення 15.06.2024)

6. Звіт компанії cloudflare про DDoS–атаки та їх загрози https://blog.cloudflare.com/ddos–threat–report–for–2024–q1/ (дата звернення 15.06.2024)

7. Інформація про DDoS–атаки на основі DNS https://www.catchpoint.com/dns–monitoring/dns–flood#:~:text=DNS%20flood%3A%20A%20DNS%20DDoS&text=In%20a%20DNS%20flood%20attack,Internet%20speeds%2C%20and%20other%20disruptions. (дата звернення 15.06.2024)

8. Ризики з якими стикається малий бізнес https://www.ondeck.com/resources/risks–small–businesses–face–and–how–to–avoid–them (дата звернення 15.06.2024)

9. Інформація про внутрішні та зовнішні загрози https://www.securonix.com/blog/shifting–perceptions–of–insider–threats–vs–external–cyber–attacks/ (дата звернення 16.06.2024)

10. Статистичні дані про інсайдерські загрози для малих компаній https://www.tessian.com/blog/insider–threat–statistics/ (дата звернення 16.06.2024)

11. Закон про інформацію https://zakon.rada.gov.ua/laws/show/2657–12#Text (дата звернення 16.06.2024)

12. НД ТЗІ 1.4–001–2000 https://tzi.com.ua/downloads/1.4–001–2000.pdf (дата звернення 16.06.2024)

13. Закон України про захист інформації у ІКС https://zakon.rada.gov.ua/laws/show/80/94–%D0%B2%D1%80#Text (дата звернення 14.06.2024)

14. НД ТЗІ 2.5–004–99 https://tzi.com.ua/downloads/2.5–004–99.pdf (дата звернення 14.06.2024)

15. НД ТЗІ 1.1–003–99 https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення 14.06.2024)

16. НД ТЗІ 1.1–002–99 https://tzi.com.ua/downloads/1.1–002–99.pdf (дата звернення 14.06.2024)

17. Закон України про державну таємницю https://zakon.rada.gov.ua/laws/show/3855–12#Text (дата звернення 14.06.2024)

18. ДСТУ ISO/IEC 27001:2015 https://www.assistem.kiev.ua/doc/dstu_ISO–IEC_27001_2015.pdf (дата звернення 14.06.2024)

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	9	
6	А4	2 Розділ	26	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	2	

ДОДАТОК Б. Перелік документів на оптичному носії

Кваліфікаційна робота Гапончук А.В._125-20-2.pdf

Презентація Гапончук Антон.pptx

ГапонукАВ_125-20-2_Кр.pdf

ДОДАТОК В. Відгуки керівників розділів

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б.

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2
Гапончука Антона Володимировича
на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ ArchBuild»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 64 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захисту інформації в ІКС ТОВ ArchBuild.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведено обстеження об'єкту інформаційної діяльності, проаналізовано та класифіковано інформацію що зберігається та циркулює на об'єкті інформаційної діяльності. Побудовано модель порушника та модель загроз. На підставі побудованих моделей було визначено актуальні проблеми у ІКС компанії та розроблено основні елементи політики безпеки.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності інформації шляхом впровадження організаційних заходів захисту.Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Гапончук А.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «74(добре)».

Керівник кваліфікаційної роботи проф. Валерій МАГРО

Керівник спец. розділу ст.викл. Дмитро ТИМОФЄЄВ

Додаток Д Наказ

Наказ №1

м. Дніпро

04.06.2024

Про створення комплексної системи
захисту інформації в автоматизованій
системі класу “3” ІТС ТОВ ArchBuild

На виконання вимог статті 8 Закону України ‹‹Про захист інформації в інформаційно–телекомунікаційних системах›› (зі змінами) та п.16 ‹‹Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно–телекомунікаційних системах››, затверджених Постановою Кабінету Міністрів України від 26.03.2006 року №373 (зі змінами).

НАКАЗУЮ:

1.Створити комплексну систему захисту інформації в автоматизованій системі класу ‹‹3›› для обробки інформації з обмеженим доступом.

2.Відповідальному за службу захисту інформації в автоматизованій системі Іванову І.І. забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

3.Контроль за виконанням наказу покласти на керівника компанії Іванова І.І..

Директор Іван ІВАНОВ

Додаток Е Акт категоріювання

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ
Керівник установи–власника
(розпорядника, користувача)
об’єкта
_керівник_Іванов_І.І._____
___
(посада, підпис, ініціали,
прізвище)
____. ____. 20___
М.П.

АКТ
категоріювання _____ТОВ ArchBuild_____
(найменування об’єкта категоріювання)

1. Підстава для категоріювання
_____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
_____
зміна ознаки, за якою була встановлена категорія об’єкта, тощо;
_____
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання
_____первинне_____
(первинне, чергове, позачергове)
_____
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється ____обробка інформації технічними засобами_____

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті

конфіденційна інформація

(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія 4 категорія, до четвертої категорії належать об'єкти інформаційної діяльності у яких циркулює службова та конфіденційна фнформація

Голова комісії _____ _____
(підпис) (ініціали, прізвище)

Члени комісії: _____ _____
(підпис) (ініціали, прізвище)

____.____. 20___