Хмельницький національний університет
Факультет програмування та комп'ютерних
і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів
Назва теми

КвРКБ. 170152.17.01.13. ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *Кібербезпека*

Виконав студент IV курсу, група КБ-17-1 _____ В.Ю. Пічура
Підпис Ініціали, прізвище

Керівник _____ В.Ю. Тітова
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки,
та комп'ютерних систем
і мереж _____ Ю.П. Кльоц
Підпис, дата Ініціали, прізвище

7 червня 2021 р.

Хмельницький, 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра кібербезпеки та комп'ютерних систем та мереж
Освітній рівень *бакалавр*
Галузь знань *12 «Інформаційні технології»*
Спеціальність *125 «Кібербезпека»*
Освітня програма *освітньо-професійна програма підготовки бакалавра*

ЗАТВЕРДЖУЮ:
Завідувач кафедри _____
_____
5. 01 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Пічурі Вадиму Юрійовичу
Прізвище, ім'я, по батькові студента

1 Тема роботи «Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів»
Керівник роботи Тітова Віра Юріївна, к.т.н, доцент
_____
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від ___ ____ 2021р. № ___
2 Строк подання студентом роботи на кафедру: _____
3 Вихідні дані до роботи системи управління інформаційною , класифікація загроз, методи оцінювання ризиків, види дестабілізуючих факторів,
_____
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз об'єкта захисту, обґрунтування вибору засобів для побудови системи безпеки, проектування системи управління безпекою, реалізація роботи
_____
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
«Загальна схема ситеми управління інформаційною безпекою», «Модель загроз», «Модель порушника», «Алгоритм розрахунку оцінки ризиків»
_____
_____

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ		
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ		

7 Дата видачі завдання 5 лютого 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Пр
1	Вибір та затвердження теми кваліфікаційної роботи.	Січень	
2	Аналіз об'єкта захисту.	Січень–лютий	
3	Проектування та розробка загальної архітектури і структури системи захисту.	Лютий–березень	
4	Програмна реалізація запропонованого рішення та тестування системи; аналіз результатів і оцінювання прийнятих рішень.	Квітень	
5	Написання тексту пояснювальної записки та розробка графічних матеріалів.	Травень	
6	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника.		
7	Оформлення кваліфікаційної роботи як документа відповідно до вимог.		
8	Отримання супровідних документів. Нормоконтроль.	Червень	
9	Підготовка до захисту та захист кваліфікаційної роботи.		

Студент _____ Ящура В.Ю.
Підпис Ініціали, прізвище

Керівник роботи _____ Муляр І.В.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів.

Автор роботи: Пічура Вадим Юрійович.

Керівник роботи: Тітова Віра Юріївна.

Обсяг – 58 с., 3 рис., 2 додатки, 27 джерел.

Графічна частина: 9 презентаційних слайдів, 3 плакати.

СИСТЕМА УРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ДЕСТАБІЛІЗУЮЧІ ФАКТОРИ, ЗАГРОЗИ, РИЗИКИ.

Метою роботи є реалізація та впровадження системи управління інформаційною безпекою, оцінка ризиків інформаційної безпеки, аналіз загроз, створення моделей загроз та порушника, розробка Політики безпеки.

У роботі був здійснений аналіз дестабілізуючих факторів на захищувану інформацію, дослідження їх впливу та наслідків на інформаційні ресурси.

В ході кваліфікаційної роботи була розроблена система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів.

Підпис студента: _____ Дата: 05.06.21р

Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
	1		Завдання на дипломний проект	1	
	2		Анотація	1	
	3	КвРКБ.170152.17.01.13 ПЗ	Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів Пояснювальна записка	1	
	4	КвРКБ.170152.17.01.13 Е8	Модель загроз Схема структурна	1	
	5	КвРКБ.170152.17.01.13 Е8	Модель порушника Схема структурна	1	
	6	КвРКБ.170152.17.01.13 Е8	Класифікація загроз Схема структурна	1	

КвРКБ.170152.17.01.13 ВП

Арк.	№ Докум.	Підп.	Дата
Розробив	Пічура В.Ю.		
Перев.	Тітова В.Ю.		
Н.контр.	Муляр І.В.		
Зав.	Кльоц Ю.П.		

Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів
Відомість проекту

Літера	Аркуш	Аркушів
и	1	1

ХНУ, КБ-17-1

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – база даних;

ЕОМ – електронно-обчислювальна машина;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

ІТ – інформаційні технології;

КС – комп’ютерні системи;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СУІБ – система управління інформаційною безпекою;

ТЗ – технічний захист;

УІБ – управління інформаційними ризиками;

ВСТУП

Для забезпечення інформаційної безпеки на сьогоднішній день важливо використовувати цілу систему засобів спрямованих на захист даних. Фактично в кожній установі циркулює величезний потік інформації, від загальнодоступної (публічної) до надсекретної. Важливо забезпечити захист інформації на усіх етапах її життєвого циклу, тобто в процесі обробки, зберігання та передачі.

Напевно, найчастіше це питання стоїть у компаній, які мають територіально розподілену інфраструктуру, тому що в них відбувається постійний та безперервний обмін даними між об'єктами мережі.

Якщо правильно спланувати та реалізувати систему захисту інформаційною безпекою, використовуючи сучасні технології та дотримуючись міжнародних стандартів, то можна максимально мінімізувати ризик загроз інформації. У поєднанні організаційних та технічних засобів.

Інформаційна безпека є дуже актуальною проблемо у сьогоденні, тому що у світі щодня збільшується кількість кіберзлочинів та кібератак. Система управління інформаційною безпекою є однією з найголовніших складових систем забезпечення захисту інформації. А основна задача інформаційного захисту вирішується внаслідок покращення процесу управління даними за допомогою реалізації всіляких підходів та методів, а також використанню організаційних засобів та дотримання нормативних вимог.

Метою кваліфікаційної роботи студентів спеціальності «Кібербезпека» являється закріплення та підтвердження знань, які були отримані у процесі навчання на попередніх курсах, набуття практичних навичок проєктування, моделювання та дослідження інформаційних управляючих систем за допомогою сучасних програмних засобів та технологій.

Завдання кваліфікаційної роботи:

- систематизація, закріплення, розширення та застосування теоретичних знань і практичних навиків з дисциплін;

- розвиток та закріплення навиків самостійної роботи;

- удосконалення вміння користуватись сучасними системами програмування, вирішувати інженерні задачі з проектування захищених інформаційних систем та їх елементів, використовуючи сучасні методології, інформаційні технології, здійснювати комп'ютерне моделювання, а також обробляти і систематизувати результати досліджень, використовуючи відповідні інструментальні засоби.

1 АНАЛІЗ ОБ'ЄКТА ЗАХИСТУ

1.1 Поняття системи управління інформаційною безпекою

Для того, щоб забезпечити необхідний рівень інформаційної безпеки на різних підприємствах, установах створюються системи управління інформаційною безпекою (СУІБ).

Основною метою створення СУІБ являється запобігання та мінімізація шкоди, яка здійснюється шляхом небажаного впливу на ресурси та компоненти інформаційної системи (ІС). Таким чином, система управління інформаційною безпекою є частиною загальної системи управління організації, на основі оцінки ділового ризику вона створює, впроваджує, експлуатує, контролює, підтримує та вдосконалює рівень інформаційної безпеки.

СУІБ включає в себе:

- організаційну структуру
- політики ІБ
- посадові обов'язки
- планування
- процеси
- процедури
- ресурси [1]

Головне завдання СУІБ – забезпечити необхідний рівень доступності, цілісності та конфіденційності інформаційних ресурсів.

Об'єктами управління інформаційної безпеки є інформаційні ресурси та ІС.

Інформаційний ресурс – це інформація, яка подана у вигляді записаних інформаційних масивів чи баз даних, які потребують захисту[2].

Інформаційна система – це сукупність взаємопов’язаних інструментів, методів та персоналу, що використовуються для досягнення поставленої мети при збереженні, обробці, передачі та прийому інформації [3].

Інформаційна безпека в ІС є однією з основних сфер безпеки країн, галузей, відомств, державних організацій чи приватних компаній.

СУІБ складається з політики, процедур, керівних принципів та відповідних ресурсів, якими організація спільно керує для захисту своїх інформаційних активів. СУІБ визначає систематичний метод створення, впровадження, обробки, контролю, перегляду, підтримання та вдосконалення ІБ організації для досягнення бізнес-цілей.

Вона основана на оцінці ризиків в організації та допустимих рівнях ризику, і спрямований на ефективне управління та управління ризиками. Аналіз вимог щодо захисту інформаційних активів та вжиття відповідних захисних заходів для забезпечення необхідного захисту цих активів допоможе успішно впровадити СУІБ. Наступні основні принципи сприяють успішному впровадженню СУІБ:

- усвідомлення необхідності системи ІБ;
- поєднання управлінських обов'язків з інтересами зацікавлених сторін;
- розвиток соціальних цінностей;
- оцінка ризику для визначення відповідних захисних заходів для досягнення прийнятного рівня ризику;
- безпека як важлива частина ІС та мереж;
- активне запобігання та виявлення інцидентів інформаційної безепеки;
- постійна переоцінка та відповідне покращення ІБ.

Для процесів СУІБ застосовують цикл Шухарта-Демінга, або ж його друга назва - модель «PDCA», яка зображена на рисунку 1.1.

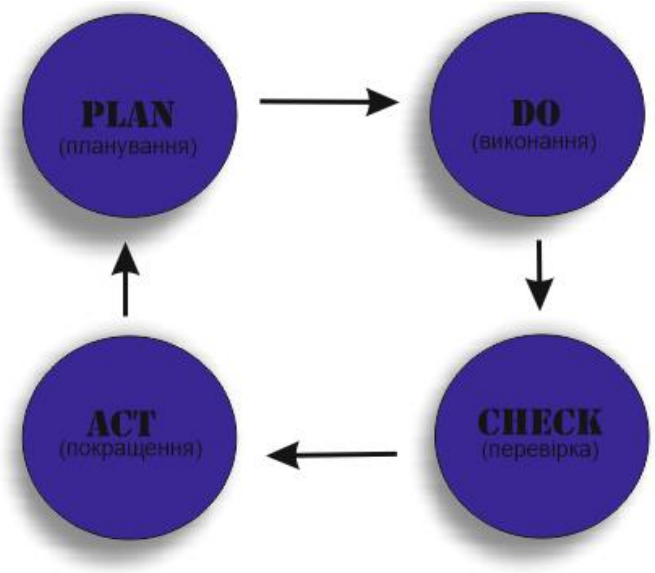


Рисунок 1.1 – модель «PDCA»

1. Планування – на цьому етапі відбувається розроблення політики безпеки, визначення цілей, процесів і процедур, які пов’язані з управлінням ризиками та підвищенням рівня інформаційної безпеки, для того щоб досягнути результатів поставлених організацією.

2.Виконання – впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю .

3. Перевірка – оцінка результативності виконання вимог політик, цілей ІБ і ефективності функціонування СУІБ і оповіщення вищого керівництва про результати.

4. Покращення – проведення коригувальних та запобіжних дій, заснованих на результатах аудиту та аналізу з боку керівництва для досягнення поліпшення СУІБ.

1.2 Аналіз дестабілізуючих факторів інформаційної безпеки

Дестабілізуючі фактори – явища та процеси природного і штучного походження, що породжують інформаційні загрози.[5]

Джерелами дестабілізуючих факторів можуть виступати будь хто, від звичайної людини до різних установи чи чи компаній. Найсильнішими з них є ворожі країни, у них зазвичай створюються і функціонують спеціальні органи та служби для формування інформаційних загроз.

Інормаційні ситеми та засоби також складають певну групу джерел, адже вони приводять в дію інформаційні загрози та виступають чинником різних загроз, наприклад, через несправність.

Навіть природа може виступати джерелом дестабвлізуючих факторів. Стихійні лиха, атмосферні явища так чи інакше можуть бути потенційними загрозами для іфнормаційної безпеки.

Дестабілізуючі фактори умовно можна поділити на міждержавні та внутрішньодержавні. Сукупність джерел та дестабілізуючих факторів створюють низку інформаційних загроз, які впливають на стан свідомості окремих людей, суспільства та країни. До них належать: крадіжка, знищення, втрата, модифікація, розголошення, підробка, витік правдивої (істинної) інформації, та підробка, розповсюдження та впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів належать:

- правовий вакуум у більшості питань забезпечення інформаційної безпеки;
- навмисне/ненавмисне порушення законодавства з питань інформаційної безпеки;
- політичні конфлікти;
- зловмисні дії злочинних елементів або груп;
- відмови, збої, технічні помилки інформаційних систем;
- природні явища, які ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.[6]

Міждержавні дестабілізуючі фактори — це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т. ін.)[7]

Серед усіх джерел інформаційних загроз найпоширенішим та найбільш небезпечним були, є і залишаться люди. На підприємствах їх класифікують наступним чином:

- працівники даної установи;
- третя сторона(постачальники, підрядники, партнери) ;
- контролюючі органи;
- зловмисники, хакери.

Занепокоєння підприємств з приводу того, що працівники сприяють ризикам інформаційної безпеки не є безпідставними. Співробітники можуть допускати помилки, які піддають ризику дані або системи їх компанії, наприклад, через необережність може статись випадковий витік даних, або ж причина може бути в тому, що вони не мають необхідної підготовки у роботі з обладнанням та програмним забезпеченням.

Людські помилки з боку персоналу не єдиний «вектор атаки», жертвами якого стає бізнес. Коли в бізнесі трапляються інциденти з безпекою, важливо, щоб співробітники були готові або помітити порушення, або зменшити ризики. Зрештою, хоча співробітники можуть становити ризик для компаній, вони також повинні відігравати важливу роль, допомагаючи захистити компанію.

Однак співробітники не завжди вживають заходів, коли їхня компанія потрапляє в аварію безпеки. На більшісті підприємств у всьому світі працівники приховують інцидент, коли він трапляється.тПриховування інциденту може призвести до значних наслідків, збільшуючи завдану шкоду. Одна неповідомлена подія може навіть призвести до значного порушення всієї інфраструктури організації. Це так звання проблема «хованки».

Водночас люди є найрізноманітнішим джерелом тому, що йому, властива більша кількість видів та способів дестабілізувального впливу , в порівнянні з іншими.

Це джерело є найбільш небезпечним, оскільки воно наймасовіше, зовнішній вплив має постійний характер, його вплив може бути як умисним , так і ненавмисним, і може призвести до усіх форм вразливості інформації.

Технічні засоби та способи зв’язку для зберігання, обробки, відображення та передачі інформації є друним за величиною джерелом дестабілізуючого впливу. До цього джерела відносяться:

- засоби відеозаписуючої та відтворювальної техніки;
- засоби звукозаписуючої техніки;
- засоби радіомовлення;
- засоби телебачення;
- засоби радіо, телефонного та кабельного зв'язку;
- ЕОМ;
- копіювально-розмножувальна техніка;

До третього джерела дестабілізуючого впливу можна віднести системи електропостачання, водопостачання, теплопостачання, кондиціонування.

Четвертим джерелом являються технологічні об’єкти атомної енергетики, хімічна, електронна промисловість, а також певні об'єкти з виробництва зброї та військової техніки, які змінюють природну структуру навколишнього середовища.

П’ятим джерелом виступають природні явища , тобо урагани, цунамі, повені, вулканізм, метеоризм, селі тощо.

Залежно від джерела та його типу вплив може бути безпосереднім або опосередкованим, тобто діяти через інші джерела.

Зі сторони людей простежуються такі види впливу:

1. Вплив на носії інформації;
2. НСД та незаконне розповсюдження конфіденційної інформації;
3. Вихід з ладу обладнання;
4. Порушення режиму роботи обладнання.

До способів безпосереднього впливу можн віднести:

- фізичне пошкодження/руйнування носіїв інформації;
- знищення дпних на носіях;
- різні види розмагнічування носіїв;
- внесення підробної інформації у носії або ж її модифікація.

Безпосередній вплив на захищувану інформації здійснюється шляхом необережним та ненавмисним залишенням їх у зонах, що не охороняються, як правило, у громадському транспорті, магазинах чи на ринках, що може призвести до втрати засобів інформації.

Незаконне розповсюдження конфіденційних даних може здійснюватися шляхом:

- словесної передачі інформації;
- передачі скан-копій/фото даних;
- показу носіїв інформації;
- публікування даних в пресі чи мережі Інтернет;
- використання інформації у доповідях, що транслюються по ТБ та радіо.

Втрата носіїв важливих даних може призвести до витоку чи розголошення інформації.

Способами виведення з ладу технічних пристроїів є наступні:

- Неправильна установка пристрою;
- Поломка (пошкодження) засобів, включаючи розрив (пошкодження) кабельних ліній зв'язку;
- Створення аварійних ситуацій для обладнання;
- Відключення пристроїв від систем/живлення;
- Виведення з експлуатації або порушення режиму роботи системи для забезпечення роботи засобів;
- Вмонтування в ЕОМ засобів стеження.

Способами порушення режиму роботи обладнання можуть бути:

- пошкодження певних елементів обладнання;

- порушення правил застосування обладнання;
- зміна порядку обробки інформації;
- зараження програм обробки інформації комп'ютерними вірусами;
- видача неправильних програмних команд;
- перевищення розрахункового числа запитів;
- створення перешкод за допомогою додаткового звукового або шумового фону при передачі інформації по каналах радіозв'язку;
- передача помилкових сигналів;
- зміна режиму роботи систем, що забезпечують працеспроможність обладнання.

Одним з видів дестабілізуючого впливу є технічні засоби пов'язані з обробкою даних. До них належать:

- Виведеня з ладу обладнання;
- Технічні помилки/збої в роботі обладнання;
- Використання електромагнітного випромінювання.

Виведення з ладу технічного обладнання, що може призвести до збоїв/неможливості виконання операцій, тобто це може відбуватись через:

- Технічні помилки/аварії;
- Загоряння/затоплення;
- Вплив природних явищ або стихійних лих;
- Знищення/пошкодження носіїв інформації;
- Зараження програм для обробки вірусами;

Технічні помилки/збої в роботі можуть виникнути внаслідок:

- Технічних несправностей;
- Зараження програм для обробки даних вірусами;
- Природного впливу;
- Помилок режиму функціонування обладнання;

Останнім джерелом дестабілізуючого впливу вважаються природні явища. До них входять стихійні лиха та атмосферні явища.

Стихійні лиха і одночасно види впливу – урагани, смерчі, шторми, зсуви, селі, торнадо, повені, тощо; атмосферні явища – снігопади, дощі, перепади температури та вологості повітря, зливи, грози, магнітні бурі.

Способами впливу зі сторони природних явищ можуть бути знищення (поломки), загоряння, затоплення обладнання, систем забезпечення його функціонування, порушення режиму роботи обладнання.

Розглядаючи ознаки та складові загрози для захищеної інформації можна сказати, що в основі будь-якого дестабілізуючого впливу лежать певні причини та мотиви, що призводять до конкретних видів впливів та методів. Водночас причини виправдані – обставини або передумови, що призвели до цих факторів, сприяли їх виникненню. Однак існування джерел, типів, методів, причин,умов та наслідків дестабілізуючого впливу є потенційною небезпекою, що може виникнути тільки за умови дотримання певних правил.

1.3 Міжнародні стандарти інформаційної безпеки

Щоб чітко визначити заходи з кібербезпеки, потрібні письмові норми. Ці норми відомі як стандарти кібербезпеки: загальні набори рецептів для ідеального виконання певних заходів. Стандарти можуть включати методи, керівні принципи, довідкові рамки тощо. Це забезпечує ефективність безпеки, сприяє інтеграції та сумісності, дозволяє суттєве порівняння заходів, зменшує складність та забезпечує структуру для нових розробок.

Стандарт безпеки - це «опублікована специфікація, яка встановлює загальну мову, містить технічну специфікацію або інші точні критерії та призначена для послідовного використання, як правило, керівних принципів або визначень» [7]. Метою стандартів безпеки є поліпшення безпеки систем, мереж та критичних інфраструктур інформаційних технологій (IT). Добре написані стандарти кібербезпеки забезпечують послідовність у розробників продуктів і служать надійним стандартом для придбання продуктів безпеки.

Стандарти безпеки, як правило, передбачені для всіх організацій, незалежно від їх розміру чи галузі та сектора, в якому вони працюють. Цей розділ включає інформацію про кожен стандарт, який зазвичай визнається важливим компонентом будь-якої стратегії кібербезпеки.

ISO означає Міжнародна організація зі стандартизації. Міжнародні стандарти змушують речі працювати. Ці стандарти забезпечують специфікації світового класу на продукцію, послуги та комп'ютери для забезпечення якості, безпеки та ефективності. Вони відіграють важливу роль у сприянні міжнародній торгівлі.

Серія ISO 27000 – сімейство стандартів інформаційної безпеки, яке розроблено Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією, щоб забезпечити загальновизнану основу для найкращого управління інформаційною безпекою. Це допомагає організації захистити свої інформаційні активи, такі як дані про співробітників, фінансову інформацію та інтелектуальну власність.

Потреба у серії ISO 27000 виникає через ризик кібератак, з якими стикається організація. Кібератаки зростають з кожним днем, роблячи хакерів постійною загрозою для будь-якої галузі, яка використовує технології.

Серію ISO 27000 можна розділити на кілька типів:

ISO 27001 – цей міжнародний стандарт був підготовлений для забезпечення вимог щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою [8]. Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На створення та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги до безпеки, використовувані організаційні процеси та розмір та структура організації.

СУІБ зберігає конфіденційність, цілісність і доступність інформації шляхом застосування процесу управління ризиками та додає зацікавленим сторонам впевненість у тому, що ризики управляються належним

чином. Важливим є і те, щоб СУІБ була частиною інтегрованої з процесами організації та загальною структурою управління, і щоб інформаційна безпека враховувалась при розробці процесів, інформаційних систем та засобів управління. Цей міжнародний стандарт може використовуватися внутрішніми та зовнішніми сторонами для оцінки здатності організації відповідати власним вимогам організації щодо захисту інформації. Порядок, у якому вимоги представлені у цьому міжнародному стандарті, не відображає їх важливості та не передбачає порядку, в якому вони повинні виконуватися. Елементи списку перераховані лише для довідкових цілей.

ISO / IEC 27000 описує огляд та словниковий запас систем управління інформаційною безпекою, посилаючись на сімейство стандартів систем управління інформаційною безпекою, із пов'язаними термінами та визначеннями [8].

ISO 27000 – цей стандарт надає пояснення термінологій, що використовуються в ISO 27001 [8].

ISO 27002 – цей стандарт надає настанови щодо організаційних стандартів захисту інформації та практики управління інформаційною безпекою. Він включає вибір, впровадження, функціонування та управління засобами контролю з урахуванням середовища (ризиків) інформаційної безпеки організації. Організації, які приймають ISO / IEC 27002, повинні оцінювати власні інформаційні ризики, уточнювати свої цілі контролю та застосовувати відповідні засоби контролю (або взагалі інші форми лікування ризиків), використовуючи стандарт для керівництва.

ISO 27005 – цей стандарт підтримує загальні концепції, зазначені в 27001. Він призначений для надання вказівок щодо впровадження інформаційної безпеки на основі підходу до управління ризиками. Для повного розуміння ISO / IEC 27005 потрібно знання концепцій, моделей, процесів та термінологій, описаних у ISO / IEC 27001 та ISO / IEC 27002. Цей стандарт

підходить для всіх видів організацій, таких як неурядові організації, державні установи та комерційні підприємства.

ISO 27032 – це міжнародний стандарт, який чітко фокусується на кібербезпеці. Цей стандарт включає вказівки щодо захисту інформації за межами організації, наприклад, у рамках співпраці, партнерських відносин чи інших заходів щодо обміну інформацією з клієнтами та постачальниками.

Окрім сімейства стандартів ISO існують і інші:

Національний інститут стандартів і технологій (NIST)

NIST - це лабораторія вимірювальних стандартів та нерегулююча установа Міністерства торгівлі США. Його місія - сприяти інноваціям та промисловій конкурентоспроможності.

Британський інститут стандартизації (BSI)

BSI є національним органом стандартизації Великобританії. BSI виробляє декілька технічних стандартів на широкий спектр продуктів та послуг, а також постачає сертифікацію та послуги, пов'язані зі стандартами, для підприємств.

Маючи глибокі знання ISO / IEC 27001, BSI не тільки допомагає вдосконалювати їх, але також надає послуги, які навчають та сертифікують незліченні організації по всьому світу для впровадження ефективних ISO / IEC 27001 СУІБ.

Робоча група з питань Інтернет-інженерії (IETF)

IETF - це організація з відкритими стандартами, яка не вимагає офіційного членства та вимог до членства. IETF створює та просуває добровільні стандарти Інтернету, зокрема стандарти для набору протоколів Інтернету (TCP / IP) [9].

IETF організований у кілька робочих груп, зосереджених на тематиці. Поточні галузі включають програми, Інтернет, операції та управління, програми та інфраструктуру в режимі реального часу, маршрутизацію, транспорт та, цілком очевидно, безпеку.

Рада зі стандартів безпеки платіжних карток (PCI SSC)

PCI SSC - це глобальний відкритий орган, відповідальний за створення, вдосконалення, розповсюдження та допомогу в розумінні стандартів безпеки для захисту платіжних рахунків [10].

Стандарт безпеки даних платіжних карток (PCI DSS) був розроблений як засіб посилення контролю за безпекою даних власників карток та зменшення ризику шахрайства з кредитними картками. Це вимагає щорічної перевірки відповідності, що проводиться або зовнішнім кваліфікованим оцінювачем безпеки (QSA), або спеціальним оцінювачем внутрішньої безпеки, який створює звіт про відповідність для організацій, що здійснюють великі обсяги транзакцій. Для обробки менших обсягів також можна виконати анкету самооцінки (SAQ).

Хоча розуміння PCI є обов'язковим лише для компаній, які обробляють інформацію про власників карток, будь-який інженер з безпеки може скористатися знаннями стандарту, оскільки він є безкоштовним, і його цілі контролю включають відповідну інформацію для захисту будь-якої компанії.

1.4 Управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки – це процес управління ризиками, пов'язаними з використанням інформаційних технологій [11]. Він включає виявлення, оцінку та лікування ризиків для конфіденційності, цілісності та доступності активів організації. Кінцевою метою цього процесу є лікування ризиків відповідно до загальної толерантності до ризиків в організації. Підприємства не повинні розраховувати на усунення всіх ризиків; швидше, вони повинні прагнути визначити та досягти прийнятного рівня ризику для своєї організації.

Етапи системи управління інформаційними ризиками:

Визначення активів: які дані, системи чи інші активи вважатимуться цінними даними організації.

Визначення вразливостей: які вразливості на системному рівні чи програмному забезпеченні ставлять під загрозу конфіденційність, цілісність та доступність активів.

Визначення загроз: які є потенційні причини компрометації активів чи інформації. Моделювання загроз - це важлива діяльність, яка допомагає додати контекст, пов’язуючи ризики з відомими загрозами та різними способами, за допомогою яких ці загрози можуть спричинити реалізацію ризиків за допомогою використання вразливостей.

Визначення елементів керування: що підприємство має для захисту ідентифікованих активів. Елемент управління безпосередньо звертається до виявленої вразливості або загрози, або повністю виправляючи її (виправлення), або зменшуючи ймовірність та / або вплив реалізованого ризику (пом'якшення).

Оцінка – це процес об’єднання зібраної інформації про активи, вразливості та засоби контролю для визначення ризику [13].

Після оцінки та аналізу ризику організації потрібно буде вибрати варіанти виправлення:

- Санація : впровадження контролю, який повністю або майже повністю фіксує основний ризик.
- Пом'якшення наслідків : зменшення ймовірності та / або впливу ризику, але не повне його фіксування.
- Передача: передача ризику іншому суб’єкту господарювання, щоб ваша організація могла оговтатися від понесених витрат, пов’язаних із реалізацією ризику.
- Прийняття ризику: Не фіксуючи ризик. Це доцільно у випадках, коли ризик явно низький, а час та зусилля, необхідні для встановлення ризику, коштують більше, ніж витрати, які виникли б у разі реалізації ризику.
- Уникнення ризику: видалення всіх випадків виявлення ризику.

Управління ризиками є постійним завданням, і його успіх зведеться до того, наскільки добре оцінюються ризики, повідомляються плани та

виконуються ролі. Визначення критично важливих людей, процесів та технологій, які допоможуть виконати наведені вище кроки, створить міцну основу для стратегії та програми управління ризиками у вашій організації, яку з часом можна розвивати.

2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ДЛЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ

2.1 Методи забезпечення інформаційної безпеки

Діяльність, яка пов’язана із забезпеченням інформаційної безпеки реалізовується за допомогою різних технологій, засобів та прийомів, що в сукупності складають методи. Метод передбачає певний набір дій на основі конкретного плану. Залежно від типу та обсягу використовуваної діяльності, методи можуть сильно відрізнятися. Важливими методами аналізу стану інформаційної безпеки являються методи їх опису та класифікації Для того, щоб ефективно захистити СУІБ потрібно, необхідно описати та класифікувати різні типи загроз та ризиків, ризиків та викликів, а потім створити систему дій для їх реалізації.

Як загальний метод аналізу рівня інформаційної безпеки використовується традиційний метод дослідження зв'язку. Ці методи розкривають причинно-наслідковий зв’язок між загрозами та ризиками, прагнуть до глибинних причин, що ведуть до конкретних факторів ризику, та розробляють дії щодо їх усунення. Такими причинно-наслідковими методами є метод подібності, метод різниці, поєднання методів подібності та відмінності, метод супутніх змін та залишковий метод.

Вибір методів аналізу СУІБ залежить від конкретного рівня та сфери організації захисту. Відповідно до загроз можна виділити різні рівні загроз та різні рівні захисту. Існує кілька груп методів захисту, серед яких:

- Перешкоди для потенційного зловмисника за допомогою фізичних та програмних засобів.
- Управління або вплив на елементи захищеної системи.
- Маскування або перетворення даних із використанням криптографічних методів.

- Регулювання або розробка законодавства та комплексу заходів, спрямованих на заохочення належної поведінки користувачів, що працюють з базами даних.
- Застосування або створення умов, за яких користувач буде змушений дотримуватися правил поводження з даними.
- Заохочення або створення середовища, яке спонукає користувачів діяти належним чином.

Кожен метод реалізований різними засобами. Основними є організаційно-технічні засоби.

Розробка організаційних засобів повинна виконуватись відділами інформаційної безпеки на підприємствах. Основними завданнями такого відділу є:

- Розробити внутрішню документацію, яка визначає правила роботи з комп'ютерною технікою та конфіденційною інформацією;
- Проводити інструктаж та періодичні перевірки персоналу;
- Ініціювати підписання додаткових угод до трудових договорів, де окреслюється відповідальність за розголошення або зловживання робочою інформацією;
- Розмежувати обов'язки, щоб уникнути ситуацій, коли один працівник має у своєму розпорядженні найважливіші файли даних;
- Організувати роботу із загальними програмами робочого циклу та забезпечити збереження важливих файлів в хмарних сховищах;
- Інтегрувати програмні продукти, які захищають дані від копіювання або знищення будь-яким користувачем, включаючи керівництво компанії;
- Розробити плани відновлення системи на випадок відмов з будь-якої причини.

Група технічних засобів поєднує апаратні та програмні засоби. До основних належать:

- Регулярне резервне копіювання та віддалене зберігання найважливіших файлів даних у комп’ютерній системі;
- Дублювання та резервне копіювання всіх мережевих підсистем, важливих для безпеки даних;
- Можливість перерозподілу мережевих ресурсів на випадок несправностей окремих елементів;
- Можливість використання резервних систем живлення;
- Забезпечення безпеки від пожежі або пошкодження водою;
- Встановлення вдосконалених продуктів, які захищають бази даних та іншу інформацію від несанкціонованого доступу.

Комплекс технічних заходів включає заходи, що роблять засоби комп’ютерної мережі фізично недоступними, наприклад, обладнання приміщень камерами та сигналізацією.

Ідентифікація та автентифікація використовуються для запобігання несанкціонованому доступу до інформації.

Ідентифікація - це присвоєння унікального імені чи зображення користувачеві, який взаємодіє з інформацією [14].

Аутентифікація - це набір методів, що використовуються для перевірки відповідності користувача авторизованому зображенню [14].

Аутентифікація та ідентифікація призначені для надання або заборони доступу до даних. Автентичність встановлюється трьома способами: програмами, обладнанням або людиною. Окрім того, що особа є об’єктом автентифікації, вона може поширюватися на обладнання (комп'ютер, монітор та носії) або дані. Встановлення пароля - найпростіший спосіб захисту.

Шифрування. Захищає конфіденційність інформації. Коли дані шифруються, дані шифруються таким чином, що їх може декодувати лише одержувач. Шар Secure Sockets (SSL) , зберігає цілісність даних шляхом шифрування інформації в процесі передачі. Якщо до інформації, що надсилається, застосовано шифрування та дайджести повідомлень, одержувач

може визначити, що інформація не була підроблена під час передачі. Шифрування атрибутів підтримує цілісність даних, шифруючи збережену інформацію.

Управління доступом. Пристосовує права доступу, що надаються різним користувачам каталогів, та забезпечує засіб визначення необхідних облікових даних або атрибутів прив'язки.

Аудит. Дозволяє визначити, чи не порушена безпека вашого каталогу. Наприклад, ви можете перевірити файли журналів, що зберігаються у вашому каталозі.

Існує досить багато різних інструментів мережевої безпеки, які ви можете включити у свою лінійку послуг. Наступний перелік далеко не вичерпний, але доступні засоби захисту можуть включати:

Управління доступом. Це стосується контролю, які користувачі мають доступ до мережі або особливо чутливих розділів мережі. Використовуючи політики безпеки, ви можете обмежити доступ до мережі лише розпізнаним користувачам та пристроям або надати обмежений доступ невідповідним пристроям або запрошеним користувачам.

Антивірусне та антивірусне програмне забезпечення. Шкідливе програмне забезпечення, або «зловмисне програмне забезпечення», є поширеною формою кібератаки, яка має різні форми та розміри. Деякі варіанти швидко видаляють файли або пошкоджують дані, тоді як інші можуть тривати бездіяльними протягом тривалого періоду часу і спокійно дозволяти хакерам зайти у ваші системи. Найкраще антивірусне програмне забезпечення буде в режимі реального часу відстежувати мережевий трафік на наявність шкідливих програм, перевіряти файли журналів активності на наявність ознак підозрілої поведінки або довгострокових закономірностей та пропонувати можливості виправлення загроз.

Безпека додатків. Кожен пристрій та програмний продукт, що використовується у вашому мережевому середовищі, пропонує потенційний

шлях для хакерів. З цієї причини важливо, щоб усі програми постійно оновлювались та виправлялись, щоб запобігти використанню вразливих місць для доступу до конфіденційних даних. Захист додатків відноситься до поєднання апаратного, програмного забезпечення та найкращих практик, які ви використовуєте для моніторингу проблем та усунення прогалин у покритті безпеки.

Поведінкова аналітика. Для того, щоб виявити ненормальну поведінку, персонал служби безпеки повинен встановити базовий рівень того, що є нормальною поведінкою для користувачів, програм та мережі даного замовника. Програмне забезпечення для поведінкової аналітики розроблено, щоб допомогти виявити загальні показники ненормальної поведінки, що часто може бути ознакою того, що сталося порушення безпеки. Маючи краще розуміння базових рівнів кожного замовника, МСП можуть швидше виявляти проблеми та ізолювати загрози.

Запобігання втраті даних. Технології запобігання втраті даних (DLP) - це ті, які заважають працівникам організації обмінюватися цінною інформацією про компанію або конфіденційними даними - мимоволі чи з ненавмисними намірами - поза мережею. Технології DLP можуть запобігати діям, які потенційно можуть піддавати дані поганим акторам поза мережевим середовищем, наприклад, завантаження та завантаження файлів, пересилання повідомлень або друк.

Розподілена відмова у наданні послуги. Розподілені атаки на відмову в обслуговуванні (DDoS) стають все більш поширеними. Вони функціонують, перевантажуючи мережу односторонніми запитами на підключення, що врешті-решт спричиняє збій мережі. Інструмент запобігання DDoS очищає вхідний трафік, щоб видалити нелегітимний трафік, який може загрожувати вашій мережі, і може складатися з апаратного пристрою, який працює для фільтрації трафіку до того, як він потрапить на ваші брандмауери.

Безпека електронної пошти. Електронна пошта є особливо важливим фактором, який слід враховувати при впровадженні мережевих інструментів безпеки. Численні вектори загроз, такі як шахрайство, фішинг, зловмисне програмне забезпечення та підозрілі посилання, можуть бути приєднані до електронних листів або включені до них. Оскільки так багато з цих загроз часто використовують елементи особистої інформації, щоб виглядати більш переконливо, важливо забезпечити працівникам організації проходження достатньої підготовки з підвищення рівня обізнаності щодо безпеки, щоб виявити, коли електронний лист є підозрілим. Програмне забезпечення для захисту електронної пошти працює для фільтрації вхідних загроз, а також може бути налаштовано для запобігання вихідним повідомленням спільного використання певних форм даних.

Брандмауери. Брандмауери - ще один загальний елемент моделі мережевої безпеки [16]. По суті, вони функціонують як ворота між мережею та Інтернетом. Брандмауери фільтрують вхідний та, в деяких випадках, вихідний трафік, порівнюючи пакети даних із заздалегідь визначеними правилами та політиками, тим самим запобігаючи доступу загроз до мережі.

Безпека мобільних пристроїв. Переважна більшість із нас мають мобільні пристрої, які несуть певну форму особистих або конфіденційних даних, які ми хотіли б захистити. Це факт, про який хакери знають і яким легко скористатися. Впровадження заходів безпеки мобільних пристроїв може обмежити доступ пристрою до мережі, що є необхідним кроком для забезпечення приватного мережевого трафіку та не витоку через вразливі мобільні з'єднання.

Сегментація мережі . Розподіл та сортування мережевого трафіку на основі певних класифікацій спрощує роботу персоналу служби безпеки, коли мова йде про застосування політик. Сегментовані мережі також полегшують присвоєння або відмову в реєстраційних даних для працівників, гарантуючи, що ніхто не отримує доступ до інформації, якою він не повинен бути.

Сегментація також допомагає секвеструвати потенційно скомпрометовані пристрої або проникнення.

Інформація про безпеку та управління подіями . Ці системи безпеки (так звані SIEM) поєднують в собі системи виявлення вторгнень на основі хоста та мережі, що поєднують моніторинг мережевого трафіку в режимі реального часу зі скануванням журналу даних історичних даних, щоб надати адміністраторам вичерпну картину всієї діяльності в мережі. SIEM подібні до систем запобігання вторгненню (IPS), які сканують мережевий трафік на підозрілу діяльність, порушення політики, несанкціонований доступ та інші ознаки потенційно зловмисної поведінки, щоб активно блокувати спроби вторгнення. IPS також може реєструвати події безпеки та надсилати повідомлення необхідним гравцям в інтересах інформування адміністраторів мережі.

Веб-безпека. Програмне забезпечення веб-безпеки має кілька цілей. По-перше, це обмежує доступ до Інтернету для співробітників з метою запобігання їм доступу до сайтів, які можуть містити шкідливе програмне забезпечення. Він також блокує інші веб-загрози та працює для захисту веб-шлюзу клієнта.

3 ПРОЕКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1 Опис функціонування системи, побудова цільової функції

СУІБ, грунтується на міжнародних стандартах серії ISO, вона є перспективною та допомагає інформаційним системам установ різних рівнів та масштабів вирішити проблеми, пов'язані з відповідністю ІБ законодавству, а також нормативним актам. До найбільш важливих стандартів інформаційної безпеки в галузі УІБ відносяться :

- стандарти безпеки КС
- європейські стандарти безпеки ІТ
- канадські стандарти безпеки КС
- загальні стандарти безпеки ІТ
- стандарти сімейства ISO

У них чітко визначена важливість процесу управління ризиками та основні методи, а також включають в себе процес створення, впровадження, використання, контролю, перевірки, підтримання та вдосконалення системи інформаційної безпеки установи.

Для того, щоб підприємство ефективно працювалопотрібно проводити ідентифікацію та управляти великою кількістю процесів, основним є управління ризиками інформаційної безпеки. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання максимальної економічної ефективності з відомим та прийнятним рівнем ризику та надає керівникам різних рівнів зрозумілий метод організації та пріоритизації ресурсів з обмеженим доступом для реалізації управління ризиками.[18]

Впровадження управління ризиками безпеки дає змогу компаніям, мають розподілені корпоративні мережі використовувати економічно ефективні засоби контролю, які знижують ризик. Визначення прийнятного ризику та

методи управління ризиками залежать від багатьох факторів, наприклад, від структури певної ІС та її розподіленості, тому що різні установи використовують різні моделі, так як не істує одного загального рішення. Кожна модель забезпечує своє поєднання точності, витрачених ресурсів та часу, складності і суб'єктивності. Інвестиції у процеси УР базуються на перевірених концепціях, чіткому розприделенні ролей та обов'язків. Крім цього, ефективний план УР дасть змогу корпоративним мережам забезпечити дотримання законодавства, щоб гарантувати, що інформаційна безпека досягне належного рівня.

Оцінка ризиків підприємтсва виступає першим етапом в розробці та впровадженні СУІБ. В процесі оцінювання ризиків проводиться ідентифікація загрози активам, дається оцінка вразливостям та ймовірності виникнення загроз. Далі запропоновано алгоритм управління ризиками інформаційних активів.

Схема розрахунку ризиків зображена на рисунку 3.1:

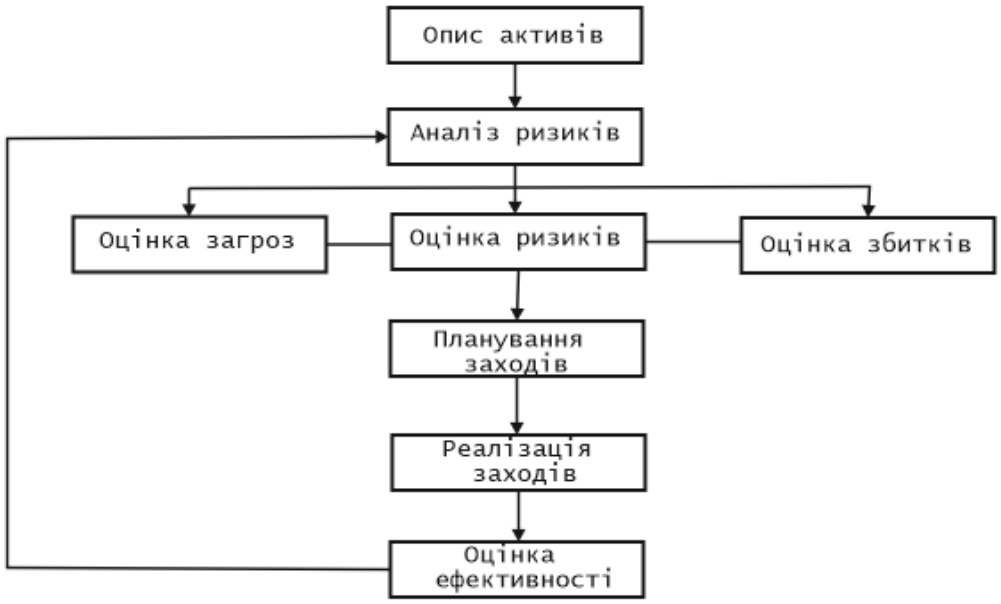


Рисунок 3.1 – Алгоритм розрахунків ризиків

Відповідно до вимог, які встановленні процесом оцінки ризиків відповідно до стандарту ISO 27002 потрібно обрати та втановити завдання та

засоби управління. Впровадження такого алгоритму дасть змогу підвищити ефективність і надійність СУІБ.

Мета створення системи управління інформаційної безпеки – зменшення матеріальних витрат, які пов’язані з порушенням ІБ. На основі даного алгоритму була розроблена узагальнена системи управління інформаційною безпекою(рисунок 3.2):

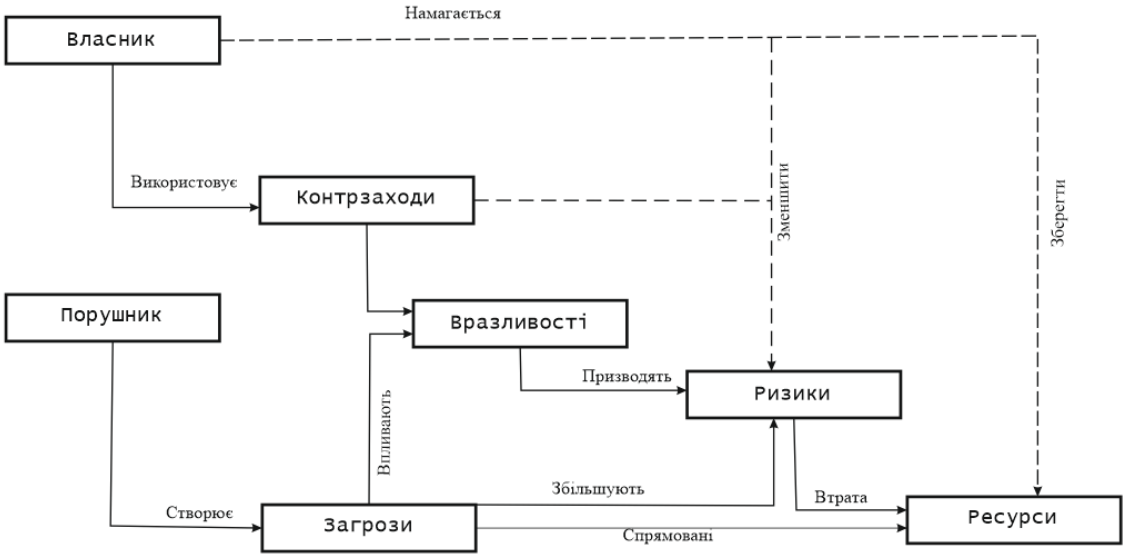


Рисунок 3.2 – Загальна схема системи управління інформаційною безпекою

Першим кроком до успішного впровадження СУІБ є усвідомлення ключовими зацікавленими сторонами необхідності інформаційної безпеки. Без участі людей, які впроваджуватимуть, контролюватимуть або підтримуватимуть СУІБ, буде важко досягти та підтримувати рівень ретельності, необхідний для створення та підтримки сертифікованої СУІБ.

Для того, щоб СУІБ організації був ефективним, вона повинна аналізувати потреби в безпеці кожного інформаційного активу та застосовувати відповідні засоби контролю, щоб захистити ці активи. Не всі інформаційні активи потребують однакових засобів контролю, і немає срібної кулі для інформаційної безпеки. Інформація надходить у всіх формах та розмірах, як і елементи керування, які захищають вашу інформацію.

Впровадження СУІБ - це не проект із фіксованою довжиною. Щоб захистити організацію від загроз вашій інформації, СУІБ повинен постійно розвиватися та розвиватися, щоб відповідати швидко змінюваному технічному ландшафту. Тому постійне переоцінювання системи управління інформаційною безпекою є обов'язковим. Часто перевіряючи та оцінюючи СУІБ, організація дізнається, чи захищена їх інформація, чи потрібно внести зміни.

Чому ж, все таки важлива СУІБ? Як державні установи, так і приватні компанії, стикаються із зростаючою загрозою порушення даних. Багато атак фінансуються державами та установами, спрямованими на викрадення власної інформації та порушення безперервності бізнесу. Ці загрози конфіденційності, доступності та цілісності даних можуть призвести до повного краху бізнесу.

Загрози від кіберінцидентів спрямовані не лише на звичайні бази даних, а на інфраструктуру та виробничі процеси, що використовують цифрові технології. Насправді кожна нова технологія, запроваджена в організації, є точкою входу в кіберзлочин.

Хоча ефективне впровадження програмних рішень для кібербезпеки та засобів управління безпекою являється надзвичайно важливим, тому що вони можуть бути легко скомпрометовані слабкою фізичною безпекою або безвідповідальним працівником, який залишає ноутбук без нагляду. Ось чому для ефективного управління ризиками необхідні політика, процедури та навчання.

3.2 Модель загроз

Модель загроз – це, по суті, структуроване представлення всієї інформації, яка впливає на безпеку програми. Моделювання загроз – це процес збору, упорядкування та аналізу всієї цієї інформації. Моделювання загроз

дозволяє обґрунтовано приймати рішення щодо ризику безпеки ігформації. На додаток до створення моделі, типові зусилля з моделювання загроз також дають пріоритетний перелік покращень безпеки концепції, вимог, проекту або реалізації.

Моделювання загроз - це сімейство заходів для поліпшення безпеки шляхом визначення цілей та вразливостей, а потім визначення контрзаходів для запобігання або пом'якшення наслідків загроз для системи.

Загроза - це потенційна або фактична небажана подія, яка може бути шкідливою (наприклад, атака DoS) або випадковою (несправність пристрою зберігання даних).

Моделювання загроз - це запланована діяльність з виявлення та оцінки загроз та вразливостей додатків.

Не існує «правильного» способу оцінки простору пошуку можливих загроз. Але є кращі чи гірші способи. Спроба оцінити всі можливі поєднання загрози, атаки, вразливості та впливу часто є марною тратою часу та сил. Зауважимо, що багато автоматизованих інструментів застосовують такий підхід - збираючи багато даних та створюючи тисячі можливих загроз. Як правило, продуктивніше зосереджуватись на пошуку високоімовірних та сильних загроз.

Основний процес моделювання загроз складається з наступних загальних етапів. Процес дослідження простору пошуку є ітеративним і постійно вдосконалюється на основі того. Так, наприклад, починати з усіх можливих вразливостей, як правило, безглуздо, оскільки більшість з них не атакуються агентами загроз, захищаються захисними засобами або не призводять до наслідків. Тому, як правило, найкраще починати з факторів, які мають велике значення.

Сфера оцінки – є першим кроком розуміння того, що загроза існує. Визначення матеріальних цінностей, таких як бази даних чи конфіденційні

файли, зазвичай є простим. Зрозуміти можливості та оцінити їх складніше. Менш конкретні речі, такі як репутація та добра воля, є найважчими для вимірювання, але часто є найбільш критичними.

Визначення джерел загроз та можливі атаки. Ключовою частиною моделі загроз є характеристика різних груп людей, які можуть мати можливість атакувати вашу інформацію. Ці групи повинні включати інсайдерів та аутсайдерів, які роблять як мимовільні помилки, так і зловмисні атаки.

Визначення існуючих контрзаходів. Модель повинна включати існуючі контрзаходи.

Визначення вразливих місця та аналізування наявність нових вразливостей. Пошук здійснюється за допомогою вразливостей, які пов’язують можливі атакита негативні наслідки.

Визначення пріоритетів – це все, що стосується моделювання загроз, оскільки завжди існує багато ризиків, які просто беруть доуваги. Для кожної загрози потрібно оцінити низку факторів вірогідності та впливу, щоб визначити загальний рівень ризику або тяжкості.

Визначення контрзаходів для зменшення загрози є останнім кроком для зниження ризику до прийнятних рівнів.

Таблиця 3.1 – Модель загроз

№	Вид загроз	Можливий механізм реалізації	Джерело загрози	Наслідки
1	2	3	4	5
Загрози пов’язані з зоною ризику користувача				
1	Помилки	Виникнення помилок під час заповнення бази даних	Користувач	ц

Продовження таблиці 3.1

1	2	3	4	5
2	Крадіжка	Крадіжка кінцевого пристрою користувача	Зловмисник	д
3	Хакінг	Виконання несанкціонованих дій на кінцевому пристроєві користувача	Зловмисник	к,д
4	Зараження вірусами	Зараження пристроїв користувача шкідливим програминим забезпеченням	Зловмисник	ц
5	Соціальна інженерія	Незаконне отримання конфіденційних даних користувачів	Зловмисник	к,ц
6	Перехват	Типові помилки користувачів пов’язані зі зберіганням чи зміною персональної ідентифікації	Користувач	к,ц
Загрози природного походження				
1	Катастрофа	Пожежа, повінь, землетрус, техногенні аварії	Зовнішнє середовище	д,ц

Закінчення таблиці 3.1

1	2	3	4	5
Загрози, пов’язані з локальними мережами підприємства				
1	Шахрайство	Крадіжка особистої інформації працівників школи	Зловмисник	ц
2	Шахрайство	Незаконне використання порталу з метою введення некоректної інформації	Зловмисник, користувач	ц
3	Недоліки	Відмова в роботі на рівні веб-сервісів	Зловмисник	д
4	Підміна	Несанкціонована зміна накладних	Користувач, зловмисник	ц
5	Недоліки	Помилки в програмному забезпечені системи	Зловмисник, розробник	к,д,ц
6	Комп’ютерна неграмотність	Помилкові дії користувача	Користувач	к,д,ц
7	Шахрайство	Злочинні дії з боку працівників компанії (розголошення конфіденційної інформації, підбір даних аутентифікації)	Користувач	к,ц

3.3 Модель порушника

Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та

теоретичні можливості, апріорні знання, час і місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (далі – НСД) до роботи з включеними до складу ІТС засобами.[19]

Модель порушника призначена для визначення:

- потенційних цілей порушника та їх класифікацію за рівнями небезпечності для захищуваної інформації;
- категорій працівників, третіх осіб, корстувачів в лавах яких може бути виявлений порушник;
- здогадки про рівень порушника;
- здогадки про його потенційні дії.

Цілями порушника можуть виступати:

- одержання потрвбних дпних у необхідному обсязі;
- можливість внесення змін в інформаційні процеси залежно від мети;
- завдвння шкоди шляхом знищення матеріальних/інформаційних активів.

Загалом порушників можна поділити на 2 групи: зовнішні і внутрішні.

В свою чергу зовнішніх можна розділити ще на:

- порушників з хорошим озброєнням та технічним оснащенням, вони зазвичай діють зовні швидко та групою;
- порушників-одинаків, в більшості випадків вони не мають доступу до об’єкту та стараються діяти обережно та таємно;

Теті особи, які можуть виявитись порушниками:

- відвідувачі;
- працівники з питань забезпечення систем життєдіяльності установ;
- конкуренти під прикриттям;
- постачальники;
- контролюючі органи.

Потенційних внутрішніх порушників поділяють на:

- допоміжний персонал підприємства;

- основний персонал;
- співробітників служби безпеки.

Персонал поділається ще на такі категорії:

- користувачі системи;
- персонал з обслуговування технічних засобів;
- працівники відділу розробки ПЗ;
- технічний персонал;
- працівники служби безпеки;
- керівництво.

Існує три типи мотивів: безвідповідальність, самоствердження та корисливий інтерес.

У разі порушень, спричинених безвідповідальністю, користувачі навмисно чи випадково роблять деструктивні дії, які не мають нічого спільного з зловмисністю. Здебільшого це результат некомпетентності чи недбалості. Деякі користувачі вважають, що отримання доступу до системних даних є великим успіхом і розпочинають гру самоствердження як для себе, так і в очах своїх колег.

Порушення інформаційної безпеки може бути спричинено корисливим інтересом користувача. В такому разі це буде цілеспрямована спроба подолання системи захисту для НСД до важливої інформації.

Порушників класифікують також за рівнем знань та можливостей, місцем дії та за часом.

За рівнем обізнаності:

- має низький рівень знань, проте має навики роботи з технічними засобами;
- має середній рівень знань і володіє практичними навичками роботи з технічними засобами , та частков їх обслуговуванням;
- має досить високий рівень знань в сфері програмування, обчислювальної техніки їх проектуванняі експлуатації.

За ступенем можливостей:

- використовування лише розвідувальних методів отримання даних;
- використовування пасивних засобів;
- використовування лише штатних засобів, а також вразливості системи захисту для її обходу, застосування компактних носіїв інформації, що можуть бути незаконно винесені повз пост охорони;
- використовування методів і засобів активного.

За часом виконання:

- під час функціонування компонентів системи;
- у період непрацездатності системи;
- як у процесі функціонування/неактивності системи.

За місцем виконання:

- без доступу до контрольлваної території;
- з середиіни приміщень, проте без доступу до ТЗ;
- з робочих місць працівників;
- з доступом до баз даних тп ПЗ;
- з доступом до управління засобами ІБ.

Також розглядаються такі обмеження та припущення щодо характеру поведінки потенційних порушників:

- робота з підбору персоналу та заходи контролювання працівників ускладнюють ймовірність створення груп порушників;
- порушник при плануванні способів НСД приховує свої наміри від інших прицівників;
- НСД може бути наслідком людського фактору, тобто неуважності користувачів, адміністраторів, чи помилок прийнятої технології обробки інформації, та інші.

Для якісного створення моделі порушника, вважається, що зловмисник має високій рівень обізнаності в засобах захисту та вище кваліфікацію. Ця класифікація зловмисників може бути використана для оцінки ризику, аналізу

вразливості системи та ефективності існуючих та запланованих заходів захисту.

В процесі створення моделі порушника важливими пунктами мають бути наступні:

- ймовірність реалізації загрози;
- вчасне виявлення;
- дані про порушення;

Варто зазначи той факт, що фактично всі злочини здійснюються людиною. Співробітники виступають як складовою частиною ІС, так і основною причиною та рушійною силою порушень/злочинів. Отже, питання чтану захищеності ІС є питанням людських відносин і поведінки.

Таблиця 3.2 – Категорії порушників

Позначення	Категорія	Потенційний рівень загрози
П1	Системний адміністратор	5
П2	Адміністратор безпеки	5
П3	Користувачі	4
П4	Технічний персонал	2
П5	Персонал, що обслуговує технічні засоби	3
П6	Сторонні особи	1

Таблиця 3.3 – Модель порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Ефективний рівень загрози
М1	Безвідповідальність	2
М2	Корисливість	5

Таблиця 3.4 – Модель порушка за рівнем кваліфікації та обізнаності щодо програми з базами даних

Позначення	Основні кваліфікаційні ознаки порушення	Ефективний рівень загрози
К1	Не має навичок щодо користування програмою і не володіє знаннями та інформацією про порядок функціонування програми	1
К2	Має навички користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування операційних систем і ПЗ, має практичні навички роботи із засобами , які використовуються у програмі	3
К4	Володіє знаннями щодо засобів та механізмів захисту, що використовуються у програмі	5

Таблиця 3.5 – Модель порушника за показником можливостей використання засобів порталу

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
1	2	3
З1	Має фізичний доступ до даних але не є авторизованим користувачем	1

Продовження таблиці 3.5

1	2	3
З2	Має можливість запуску фіксованого набору завдань, які реалізують передбачені функції обробки інформації	3
З3	Має можливість керування функціоналом порталу, тобто конфігурує програмне забезпечення та комплекс засобів захисту	5
З4	Не має фізичного доступу до даних	1

Таблиця 3.6 – Модель порушника за часом дії

Позначення	Характеристика можливостей порушника	Ефективний рівень загрози
Ч1	Під час бездіяльності компонентів системи(у неробочий час)	4
Ч2	Під час функціонування програми	5
Ч3	Під час перерви у роботі для обслуговування чи ремонту	3

Таблиця 3.7 – Модель порушника за місцем дії

Позначення	Характеристика місця дії порушника	Ефективний рівень загрози
Д1	У приміщені офісу, але без доступу до технічних засобів програми	1
Д2	З робочих місць користувачів	5
Д3	З домашніх ПК	3

Таблиця 3.8 – Профілі можливостей порушника

на-чення	Визначення категорії	Характер дій порушника					нь загроз
		Мотив	піфікція	жливості	с дії	сце дії	
П1	Системний дміністратор	М1,М2	К4	З3	-Ч3	Д2,Д3	5
П2	дміністратор пеки порталу	М1,М2	К4	З3	-Ч3	Д2,Д3	5
П3	Користувачі	М1,М2	Т2-К4	З3	-Ч3	Д2,Д3	4
П4	Персонал магазину	М1,М2	Т1-К4	З1	-Ч3	Д2	3
П5	Технічний персонал з луговуванняте чних засобів	М1,М2	Т1-К4	З2	-Ч3	Д2	3
П6	ороннні особи	М2	Т1-К4	З4	-Ч3	Д3	1

Критерії для оцінювання наведених у таблицях:

1-низький

2-нижчий за середній

3-середній

4-вищий за середній

5-високий

3.4 Політика безпеки

Політика інформаційної безпеки умовного підприємства ТОВ «Компанія» (далі – Політика) визначає основні методи та принципи управління інформаційною безпекою в ТОВ «Компанія» (далі – Товариство).

Метою створення Політики являється втілення та ефективне існування системи управління інформаційною безпекою (далі – СУІБ), яка буде забезпечувати захист інформації та ресурсів Товариства від зовнішніх і внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями працівників Товариства, забезпечувати безперервну роботу Товариства, сприяти мінімізації ризиків операційної діяльності Товариства та створювати позитивну репутацію Товариству при роботі з клієнтами.

Товариство грунтується на ризик-орієнтовному підході, який призначений для розуміння, моніторингу та зменшення кількості ризиків ІБ.

Політика Товариства базується на міжнародних стандартах в напрямку інформаційної безпеки.

Політика повинна бути розповсюджена на все Товариство бути використаною для усіх бізнес-процесів, апаратного та програмного забезпечення Товариства та у випадках взаємодії з третіми сторонами.

Політка ІБ визначає цілі та завдання в сфері інформаційної безпеки, якими Товариство повинно керуватися в своїй діяльності.

Основні завдання СУІБ:

- пом’якшення наслідків потенційних загроз;
- досягнення бізнес-цілей Товариства за допомогою реалізації бізнес-планів;
- забезпечення дотримання вимог чинного законодавства;
- зменшення кількості потенційної шкоди від інцидентів ІБ.

Усі цілі повинні переглядатись не менше одного разу на рік на регулярній основі.

Прийнятий Товариством підхід до системи управління інформаційною безпекою означає забезпечення узгодженості процесів та дій, що виконуються в галузі безпеки:

- зі стратегією і цілями Товариства;
- з результатами аналізу оцінки можливих ризиків;
- з результатами оцінювання працездатності системи управління інформаційною безпекою;
- зі всіма тонкостями управління діяльністю та ІТ Товариства.

Усі проекти, пов'язані із впровадженням нових інформаційних технологій, відповідають політиці інформаційної безпеки.

Усі заходи інформаційної безпеки, що впливають на ключові процеси/ послуги/функції бізнес-продуктів, повинні бути схвалені представниками структурних підрозділів компанії, які відповідають за забезпечення функціонування цих процесів/послуг/продуктів.

Детальні принципи та методи інформаційної безпеки, враховуючи конкретні умови кожного вертикального поля діяльності та діяльності компанії, визначені в документах, що стосуються цієї політики, положень, процедур та інструкцій.

Ролі і обов’язки:

Генеральний директор Товариства здійснює комплексне управління інформаційною безпекою на підприємстві та визначає пріоритетний напрямок розвитку ІБ.

Директор з безпеки займається здійсненням безпосереднього керівництва процесами організації та управлінням інформаційною безпекою у Товаристві, забезпеченням контролю та слідкуванням за дотриманням всіма співробітниками встановлених вимог інформаційної безпеки.

Топ-менеджмент Товариства займається сприянням створення, впровадження, упроавління та підтримці розвитку СУІБ, забезпеченням всіма необхідними ресурсами та є відповідальним за перегляд та оновлення основних завдань СУІБ

Усі співробітники Товариства забезпечуть підтримку належного рівня інформаційної безпеки. В силу своїх службових повноважень та обов’язків співробітники повинні виконувати, а також відповідати за виконання/невиконання вимог Політики, законодавчих, регуляторних і внутрішніх правил.

Кожен з власників інформаційних активів несе відповідальність за захист конфіденційності, цілісності та доступності відповідних активів.

Треті особи, які співпрацюють з Товариством повинні сприяти діяльності, яка спрямована на досягнення та підтримку відповідного рівня ІБ Товариства у обсязі, який відповідає його службовим обов’язкам і повноваженням.

Вимоги до інформаційної безпеки:

Ця політика є такою ж, як загальна СУІБ, і повинна відповідати юридичним та нормативним вимогам компанії в галузі захисту інформації, а також контрактним зобов’язанням.

Під час прийняття на роботу (протягом періоду інструктажу) та розміщення полісу на компанії та державних ресурсах вимоги політики повідомляються працівникам компанії. Треті сторони повинні ознайомитися з

цією політикою під час підписання угод (включаючи угоди про конфіденційність).

У межах своїх службових обов'язків/повноважень працівники зобов'язані дотримуватись вимог цієї Політики і законодавчих правил, повинні нести відповідальність за їх порушення згідно чинного законодавством України.

Товариство повинно впровадити програму підвищення обізнаності працівників з питань інформаційної безпеки. План включає різні методи інформування та навчання працівників, такі як використання інформаційних бюлетенів, заміток, спеціальних зустрічей, навчання з використанням мережевих технологій тощо.

Товариство поино мати визначений процес управління безперервністю бізнесу.

Товариство формує, тестує та оновлює плани під керівництвом голови комітету, щоб забезпечити безперебійну роботу у випадку непередбачених критичних ситуацій.

Політика повинна переглядатися за потреби, але принаймні раз на рік.

Для того, щоб сформувати оцінку ефективності цього документа можуть бути використані наступні критерії:

- число працівників та інфших сторін, що мають місце у СУІБ, але не є ознайомленими з Політикою;
- відповідність СУІБ критеріям законодавства, міжнародним стандартам чи вимогам організаційних документів Товариства;
- ефективність впровадження та супроводу СУІБ;
- чіткі зобов'язань ролей впровадження та супроводу СУІБ.

У разі виникнення проблемних ситуацій, які передбачені даною Політикою, розглядаються в робочому порядку всіма зацікавленими сторонами.

4 РЕАЛІЗАЦІЯ РОБОТИ

4.1 Аналіз інформаційних активів

Інформаційними активами є будь-яка інформація, що має цінність для установи/підприємства.

Для ідентифікації інформаційних активів потрібно визначити наступні моменти:

- Інформацію, що створюється та обробляється підрозділами в електронному/паперовому вигляді;
- Місця збереження та обробки інформації: інформаційні системи, файлові сервери, локальні комп'ютери, паперові документи, тощо;
- Користувачів, що мають доступ та працюють з інформацією як всередині так і поза компанією, вказавши організації, підрозділи та посади;
- Критичність інформації для бізнесу, яка здійснюється через оцінку можливого збитку для компанії.

Інформаційні активи мають бути визначені, задокументовані та оцінені за рівнем збитку для установи.

Таблиця 4.1 – Визначення інформаційних активів, їх вразливостей та загроз.

№	Інформаційний актив	Вразливості	Загрози
1	2	3	4
1	Технічне зебезпечення (обладнання)	Відсутність пожежної сигналізації, резервних джерел електропостачання, неефективна охорона, недбалість співробітників	Кліматичні умови, крадіжка, фізичні пошкодження, поломки, збої в електроживленні, тощо

Продовження таблиці 4.1

	2	3	4
	ограмне забезпечення	Відсутність резервного опіювання, відсутність нтролю за внесення змін, відсутнє розмежування тупу, використання ПЗ не призначенням, відсутність засобів захисту	Кліматичні умови, діжка, поломки, збої електроживленні, ошкодження, НСД
	нформація на папері (документація)	едбалість співробітників, відсутність відеоспостереження	Кліматичні умови, адіжки, знищення, обка, пошкодження
	Інформація на електронних носіях	Відсутність резервного опіювання, відсутність нтролю за внесення змін, відсутнє розмежування тупу, використання ПЗ не за призначенням	Кліматичні умови, крадіжка, фізичні пошкодження, поломки, збої в ктроживленні, тощо
	Співробітники	вдалий підбір персоналу, необережнвсть співробітників	голошення, продаж, викрадення, ифікація, підробка, НСД

Для початку визначимо цінність активів (таблиця 4.2), використаємо 4-х бальну шкалу оцінювання:

1 – реалізація ризику, який спрямований на конфіденційність, цілісність та доступність активу не буде мати як таких наслідків;

2 – реалізація ризику, який спрямований на конфіденційність, цілісність та доступність активу призведе до незначних наслідків/витрат;

3 – реалізація ризику, який спрямований на конфіденційність, цілісність та доступність активу може призвести до значних фінансових витрат та наслідків;

4 – реалізація ризику, який спрямований на конфіденційність, цілісність та доступність активу може призвести до повної зупинки існування компанії та великих фінансових затрат.

Таблиця 4.2 – Шкала цінності іфнормаційних активів

ID	Активи	Конфіденційність	Цілісність	Доступність	Цінність
A	Інформація, що необхідна для реалізації бізнесу	2	4	4	4
B	Особиста інформація	3	1	1	3
C	Стратегічна інформація	2	2	1	2
D	Інформація, яка потребує багато часу для обробки	3	2	2	3
E	Апаратно-програмне забезпечення	-	3	4	4
F	Носії інформації	-	1	2	2
G	Співробітники	-	1	1	1

У таблиці 4.3 наведений список загроз та їх ідентифікатори.

Таблиця 4.3 – Ідентифікування вибірки загроз

№	Опис загрози	Ідентифікатор
1	2	3
1	Тривале використання обчислювальних ресурсів користувачами	001
2	Завантаження нештатної ОС	002
3	Приведення системи до стану «відмова в обслуговуванні»	003
4	Програмне виведення з ладу засобів зберігання, обробки /введення / виведення / передачі інформації	004
5	Втрата обчислювальних ресурсів	005
6	Форматування носіїв інформації	006
7	Втрата носіїв інформації	007
8	Розкрадання коштів зберігання, обробки та/або введення / виведення / передачі інформації	008
9	Фізичне виведення з ладу засобів зберігання, обробки та/або введення / виведення / передачі інформації	009
10	Фізичного старіння апаратних засобів	010
11	Неправомірне шифрування інформації	011
12	Поширення «Поштових черв’яків»	012
13	Надлишкове виділення оперативної пам'яті	013
14	Використання інформації ідентифікації/ аутентифікації, заданої за замовчуванням	014
15	Зміна компонентів системи	015
16	Використання вразливостей протоколів мережевого/ локального обміну даними	016

Продовження таблиці 4.3

	2	3
7	Несанкціоноване видалення захищуваної інформації	017
8	Перезавантаження апаратних та програмно-апаратних засобів обчислювальної техніки	018
9	Пошкодження системного реєстру	019
0	Подолання фізичного захисту	020
1	стосування шкідливого коду через рекламу, сервіси та контент	021
2	Маскування дій шкідливого коду	022

У таблиці 4.4 зображені результати оцінки вразливості активів для заданого переліку загроз у таблиці 4.3. Оцінювання відбувалось за 3-х більною шкалою, де:

1 – низький рівень;

2 – середній рівень;

3 – високий рівень вразливості.

Таблиця 4.4 – Оцінка вразливості інформаційних активів

ID загрози	Цінні іформаційні активи						
	A	B	C	D	E	F	G
1	2	3	4	5	6	7	8
001	-	-	-	-	2	-	-
002	1	1	1	1	3	-	-
003	-	-	-	-	2	-	-
004	-	-	-	-	3	-	-
005	2	2	2	2	1	-	-
006	-	-	-	-	-	-	-
007	1	1	1	1	1	-	-

Продовження таблиці 4.4

1	2	3	4	5	6	7	8
008	3	3	3	3	-	-	-
009	-	-	-	-	2	-	-
010	2	2	2	2	2	-	-
011	-	-	-	-	2	-	-
012	1	1	1	1	3	3	-
013	-	-	-	-	3	-	-
014	3	3	3	3	2	2	-
015	1	1	1	1	3	3	-
016	3	3	3	3	-	2	-
017	-	-	-	-	1	1	-
018	-	-	-	-	-	-	-
019	2	2	2	2	-	1	-
020	1	1	1	1	-	-	-
021	2	2	2	-	-	1	-
022	-	-	-	-	-	-	-

Завершальним етапом перед розрахунком ризиків ІБ являється оцінка ймовірності реалізації загроз ІБ, яка представлена в таблиці 4.5, де :

1 – загроза існує, але не зустрічалася в даній сфері;

2 – загроза може виникнути 2-3 рази на рік в даній сфері;

3 – загроза була реалізована;

4 – загроза виникає 2-3 рази на рік.

Таблиця 4.5 – Ймовірність реалізації загроз

ID	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022
Ймовірність																						

4.2 Оцінка ризиків інформаційної безпеки з боку дестабілізуючих факторів

Рівень ризику інформаційної безпеки для кожного окремого активу(в даному випадку найцінніших активів) установи розраховується за формулою 1, в табл. 4.6 представлений результат для активів апаратно-програмного забезпечення та критично-важливої інформації для функціонування бізнесу.

$$Р = Ц \times СВ \times Й, \quad (1)$$

де, Р – ризик, Ц – цінність інформаційних активів, СВ – степінь вразливості, Й – ймовірність виникнення загрози.

Прийнятним ризиком вважається ризик, числове значення якого коливається в проміжку від 1 до 10, то такий ризик вважається незначним і не потребує обробки.

Середній ризик – числове значення якого коливається в діапазоні від 11 до 21 рекомендований до обробки для його мінімізації.

Високий ризик – числове значення якого знаходиться в діапазоні від 22 до 64, такий ризик вважається істотним, і потребує обов’язкової обробки.

Таблиця 4.6 – Оцінка ризиків ІБ

Цінний інформаційний актив	ID загрози	Цінність (Ц)	Степінь вразливості (СВ)	Ймовірність (Й)	Ризик (Р)	Оцінказизику
Інформація, що необхідна для функціонування бізнесу	002	4	1	1	4	Низький
	014	4	2	1	8	Низький
	017	4	3	4	48	Високий
	020	4	1	3	12	Середній
	004	4	3	2	24	Високий
	005	4	1	2	8	Низький
	007	4	3	4	48	Високий
	006	4	1	3	12	Середній
	011	4	1	3	12	Середній
	021	4	2	3	24	Високий
Апаратно-програмне забезпеченя	001	4	2	2	16	Середній
	002	4	3	1	12	Середній
	013	4	2	2	16	Середній
	015	4	3	3	36	Високий
	014	4	1	1	4	Низький
	018	4	1	2	8	Низький
	020	4	2	2	16	Середній
	003	4	2	2	16	Середній
	004	4	4	2	36	Високий
	005	4	3	3	24	Високий
	006	4	2	3	24	Високий
	007	4	1	3	12	Середній
	009	4	3	2	24	Високий
	010	4	1	3	12	Середній
	022	4	1	2	8	Низький

4.3 Можливі заходи мінімізації ризиків

Припускаємо, що керівництво компанії приймає рішення мінімізувати всі ризики, оцінка яких більша 20. В таблиці 4.7 наведений перелік контрзаходів, застосувавши котрі, можна знизити ризик до низького та середнього рівня.

Таблиця 4.7 – Мінімізація ризиків

Цінний інформаційний актив	ID загрози	Ризик	Контрзаходи	Кінцевий ризик
Інформація, що необхідна для функціонування бізнесу	017	48	Створення резервних копій та система захисту від НСД	12
	004	24	Антивірусний захист, міжмережеве екранування	12
	007	48	Облік носіїв інформації	12
	021	24	Антивірусний захист, міжмережеве екранування, організаційні заходи	8
Апаратно-програмне забезпеченя	015	36	Антивірусний захист, міжмережеве екранування, організаційні заходи, система довірених завантажень	12
	004	36	Організаційні заходи, система відеонагляду, фізичний захист	12
	005	24	Міжмережеве екранування	12
	009	24	Міжмережеве екранування	12
	006	24	Відеостеження, фізичний захист, організаційні міри	8

ВИСНОВКИ

На сьогоднішній день головним продуктом на ринку являється інформація. Вона стрімко розвивається та потребує захисту, адже в боротьбі за володіння інформацією не всі використовують законні методи.

Основним завданням кваліфікаційної роботи була розробка системи управління інормаційною безпекою. В ході виконання роботи були проаналізовані міжнародні стандарти, на основі яких і була розроблена система.

Спочатку було досліджено можливі загрози для середньостатистичного підприємства, та побудувано модель загроз, визначено їх джерела. Після чого було проведено ідентифікацію активів, на основі всіх досліджень розроблено узагальнену модель управління інформаційною безпекою та політику безпеки. Був проведений розрахунок оцінки інформаційних ризиків, за результатами якої складався план заходів протидії. Після застосувань контр заходів та перерахунку оцінки ризиків, було виявлено, що заходи були адекватними, та дали позитивий результат.

Підсумовуючи роботу можу сказати, що поставленні завдання були виконані в повному обсязі. Методи застосовані у роботі були цілком доцільними.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

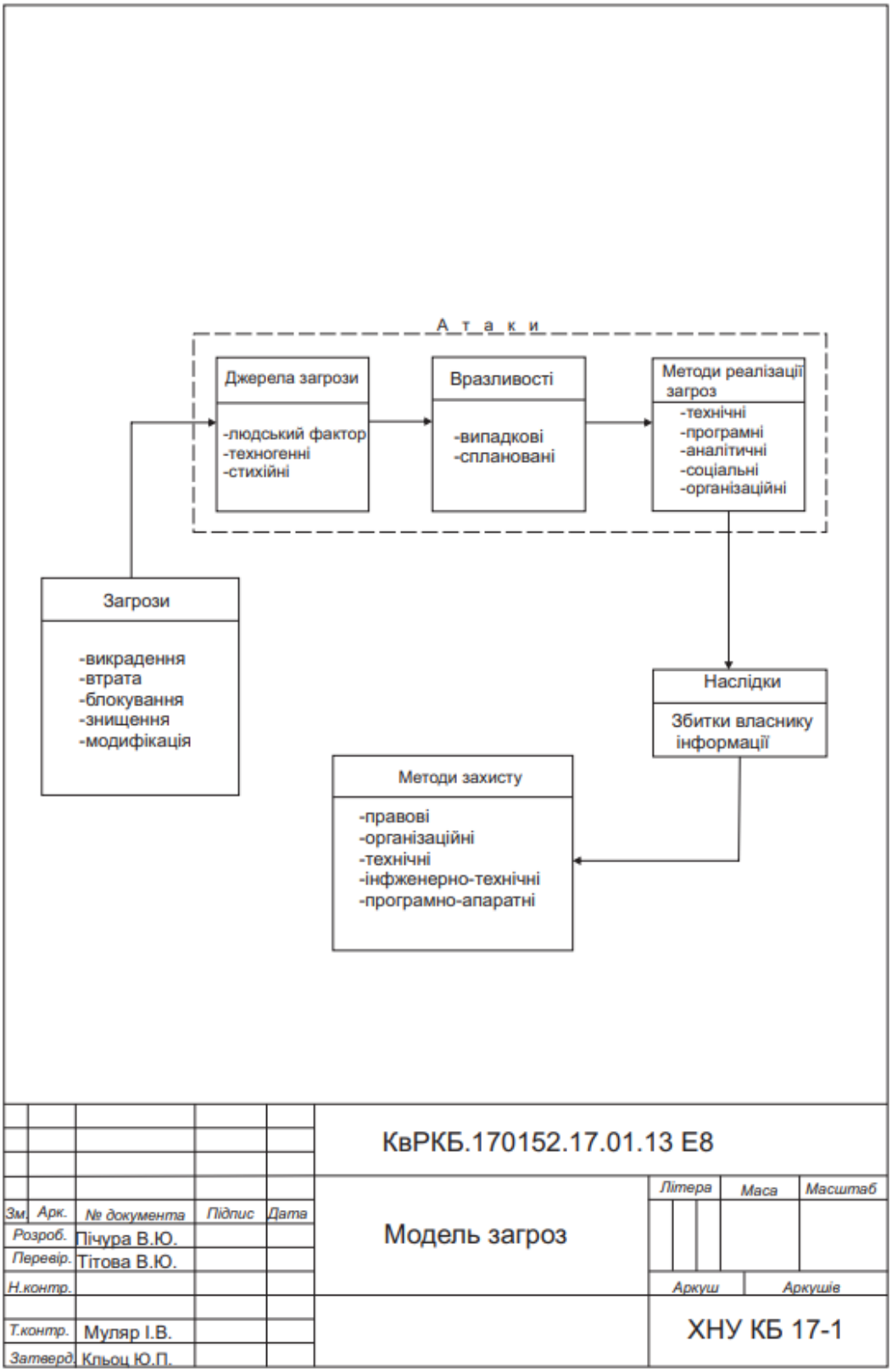
1. Основи інформаційної безпеки. [Електронний ресурс]. – Режим доступу: http://dspace.onua.edu.ua/bitstream/handle/11300/11111/%D0%9E%D0%86%D0%91%20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf?sequence=1&isAllowed=y/ (дата звернення 10.03.2021). – Назва з екрану
2. Інформаційні ресурси підприємства. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%B8/ (дата звернення 08.04.2021). – Назва з екрану
3. Інформаційні системи. [Електронний ресурс]. – Режим доступу: https://step.org.ua/konspekt/inform/tema1(дата звернення 15.04.2021). – Назва з екрану
4. Дестабілзуючі фактори інформаційної безпеки. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/informacijnabezpeka15/zagrozi-informacijnij-bezpeci/destabilizuuci-faktori-informacijnoie-bezpeki (дата звернення 19.04.2021). – Назва з екрану
5. Сучасні загрози інформаційній безпеці. [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/9973413/page:2/ (дата звернення 28.04.2021). – Назва з екрану
6. Сімейство стандартів ISO/IEC 27001. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910
7. Що таке PCI DSS і чому це потрібно кожній комерційній компанії. [Електронний ресурс]. – Режим доступу: https://www.my-itspecialist .com/uk/what-is-pci-dss-ua/ (дата звернення 11.05.2021). – Назва з екрану

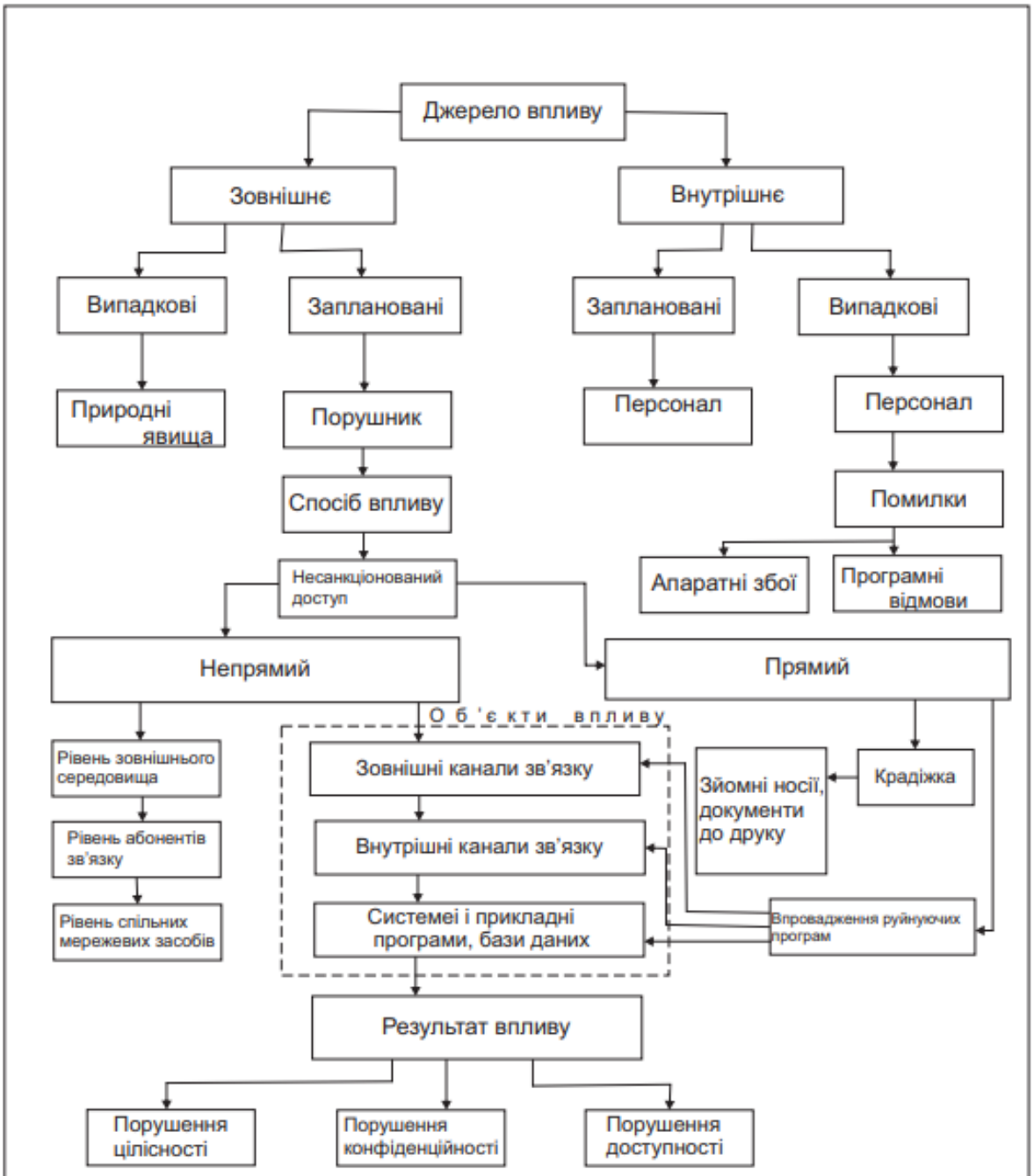
8. Управління інформаційною безпекою банку. [Електронний ресурс]. – Режим доступу: http://obt.inf.ua/page10.html
9. Поняття про ідентифікацію. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-identifikaciu
10. Управління ризиками інформаційної безпеки відповідно до ISO/IEC 27005:2018. [Електронний ресурс]. – Режим доступу: https://ua.ikmj.com/risks-management/ (дата звернення 19.05.2021). – Назва з екрану
23. Дорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно “Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)”, США, “Оранжевая книга”. – Бизнес и безопасность, 1998, № 1.
24. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. / В. В. Домарев. – К. : ТИД "ДС", 2004. – 688 с.
25. Завгородний В. И. Комплексная система защиты в компьютерных системах : Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
26. Курило А. П. Аудит информационной безопасности. / [Курило А. П., Зуфиров С. Л., Голованов В. Б. и др.]. – М. : Издательская группа "БДЦ-пресс", 2006. – 304 с.
27. Малюк А. А. Информационная безопасность : концептуальне и методологические основы защиты информации : учебное пособие для вузов. – М. : Горячая линия – Телеком, 2004. – 280 с15. Електронна комерція: Навч. посібник / А.М. Береза, І.А. Козак, Ф.А. Шевченко та ін. – К.: КНЕУ, 2002. – 326 с.

ДОДАТОК А

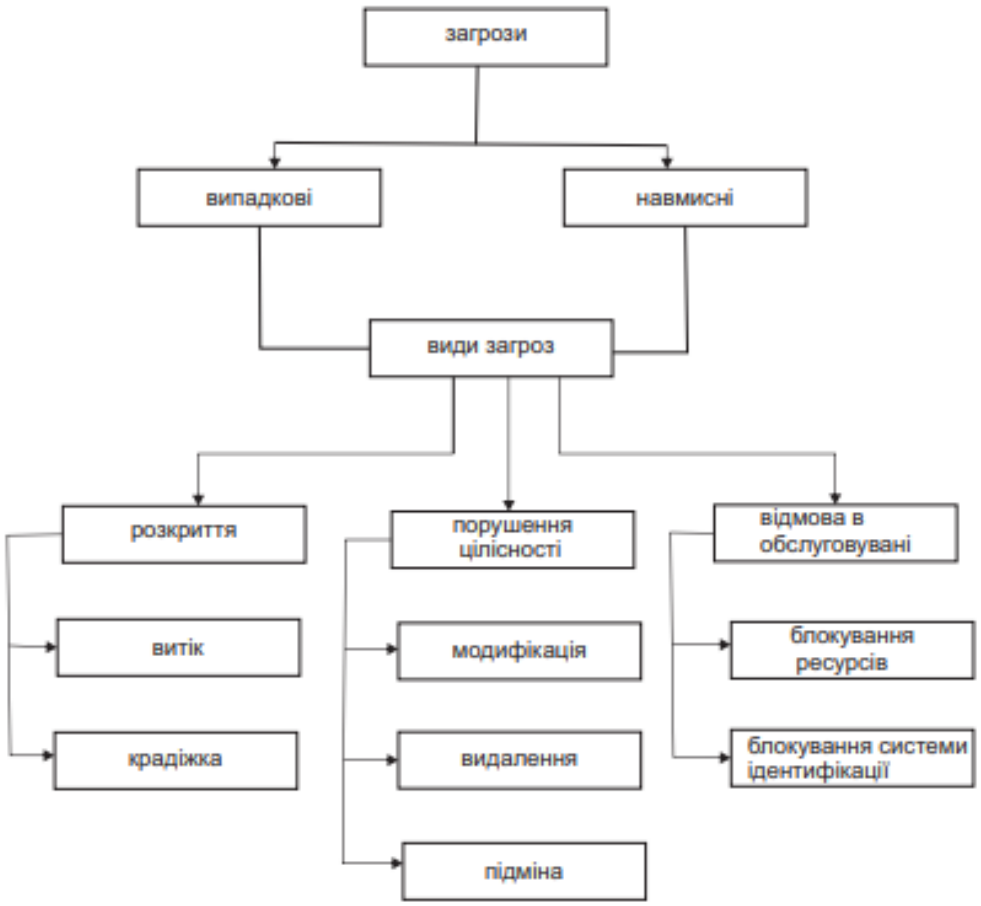
(обов’язковий)

Копія графічної частини





					КвРКБ.170152.17.01.13 Е8		
						Літера	Маса	Масштаб
Зм.	Арк.	№ документа	Підпис	Дата	Модель порушника			
Розроб.		Пічура В.Ю.						
Перевір.		Тітова В.Ю.						
Н.контр.						Аркуш	Аркушів	
Т.контр.		Муляр І.В.			ХНУ КБ 17-1			
Затверд.		Кльоц Ю.П.						



					КвРКБ.170152.17.01.13 Е8		
Зм.	Арк.	№ документа	Підпис	Дата	Класифікація загроз	Літера	Маса / Масштаб
Розроб.		Пічура В.Ю.					
Перевір.		Тітова В.Ю.				Аркуш	Аркушів
Н.контр.							
Т.контр.		Муляр І.В.				ХНУ КБ 17-1	
Затверд.		Кльоц Ю.П.					

ДОДАТОК Б

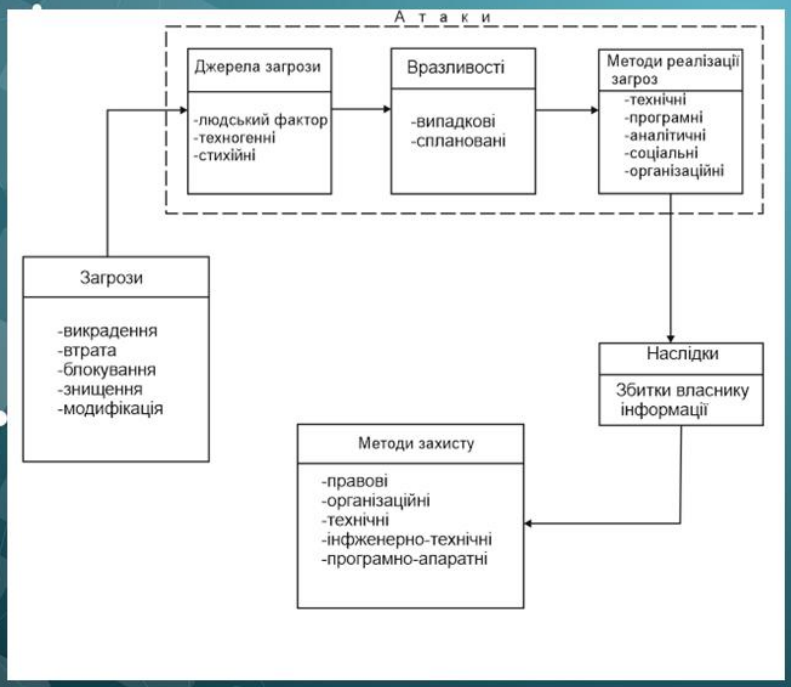
(обов'язковий)

Копія презентаційних слайдів

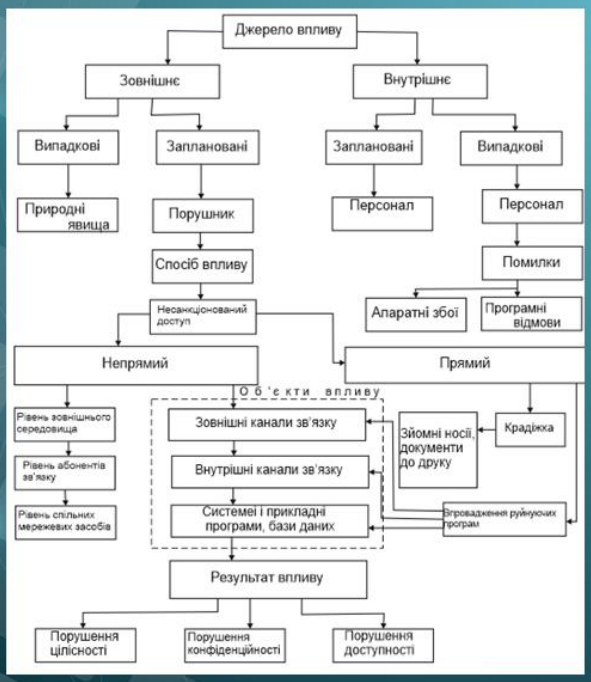
Процес створення системи управління інформаційною безпекою включає наступні пункти:

- ✓інвентаризація активів
- ✓проведення категорування активів
- ✓виявлення загроз та вразливостей
- ✓оцінення інформаційних ризиків
- ✓розробка плану управління ризиками

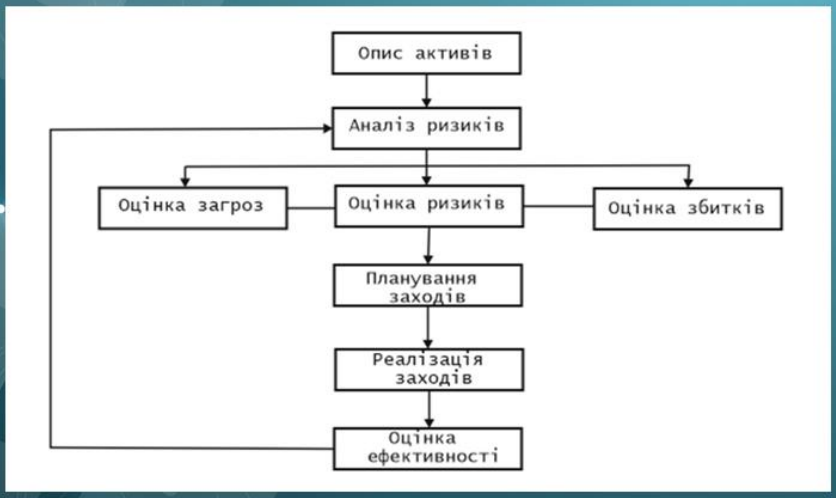
Модель загроз



Модель порушника



Алгоритм оцінювання інформаційних ризиків



Політика інформаційної безпеки

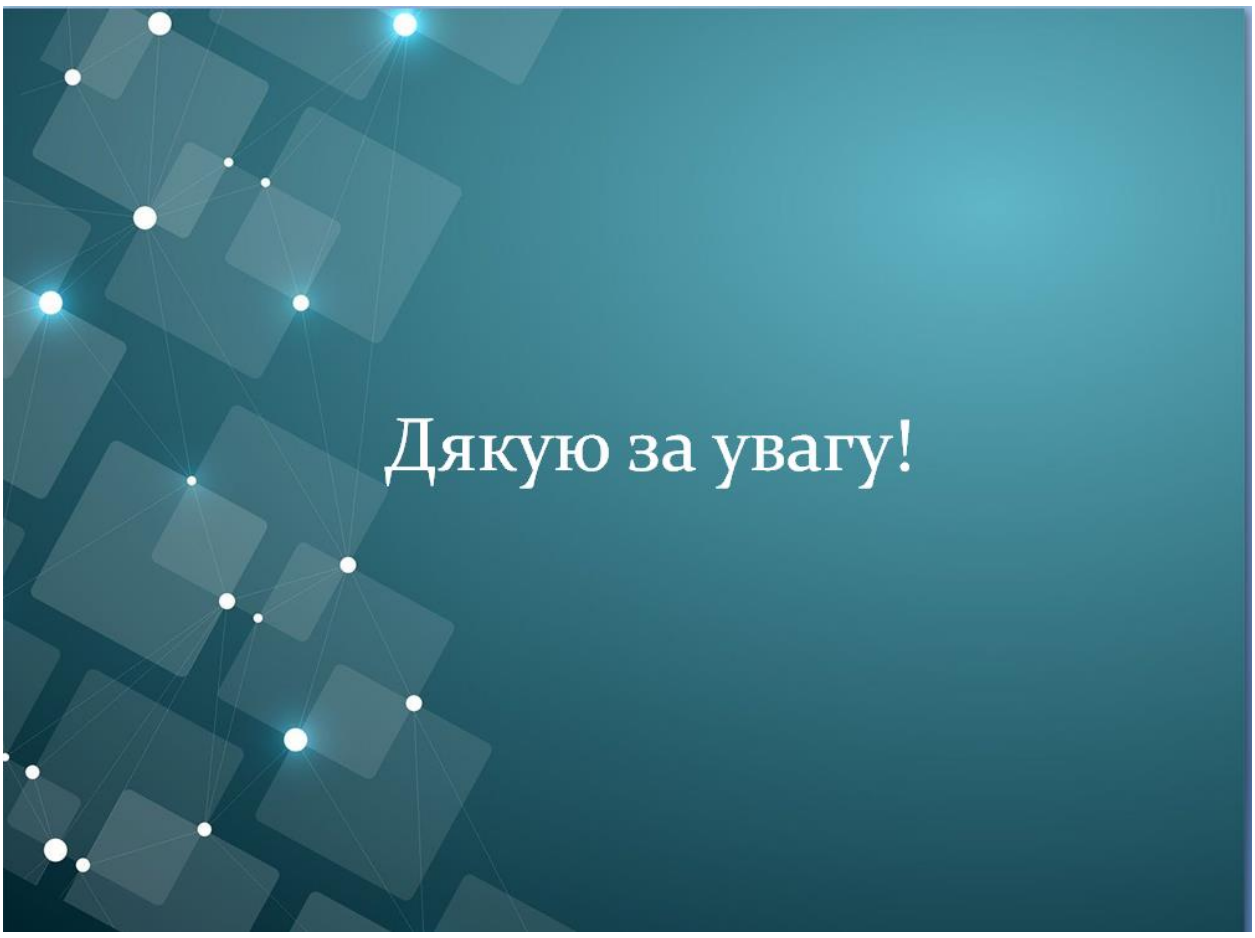
Метою створення політики інформаційної безпеки є впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на:

- захист інформаційних активів організації,
- забезпечення стабільної діяльності організації,
- мінімізації ризиків інформаційної безпеки,
- створення позитивних для організації інф. відносин з партнерами, клієнтами та всередині організації.

Основним завданням інформаційної безпеки є захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз.

Висновки

- Проведено оцінювання потенційних ризиків;
- Проведений аналіз вразливостей та загроз;
- Розроблені моделі загроз та порушника;
- Розроблена політика інформаційної безпеки;
- Вжиті заходи мінімізації потенційних ризиків.


Дякую за увагу!

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту об'єкту інформаційної діяльності ТОВ «ХмельницькІнфоком» від внутрішніх загроз

Автор: Зацепіна Орислава Олександрівна

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Керівник: Тітова Віра Юріївна, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 2,4% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.Ю. Тітова

Завідувач кафедри КбКСМ, гарант ОП _____ Ю.П. Кльоц

Дата: 07.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Пічура Вадим Юрійович

Тема Система управління інформаційною безпекою в умовах невизначеності та впливу дестабілізуючих факторів

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3 ; кількість сторінок записки 58 .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано систему управління інформаційною безпекою .

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено предмет та об'єкт дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено аналіз існуючих рішень та методів управління інформаційною безпекою, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби та методи використані для побудови системи управління. В третьому розділі визначено основні положення системи управління та розроблено алгоритми її роботи. У четвертому розділі були проведені розрахунки інформаційних ризиків та реалізовані засоби мінімізації інформаційних ризиків.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці модуля лексичного аналізу з допомогою якого визначається ступінь конфіденційності даних. На основі даного аналізу в подальшому здійснюється керуючий вплив на витік конфіденційних даних. Практична цінність результатів кваліфікаційної роботи полягає у створені системи захисту від витоків даних, що може бути підлаштована для будь якої категорії даних, і у описі оптимальних моделей функціонування систем захисту подібного характеру.

5. Негативні сторони роботи Розроблена система управління інформаційною безпекою недостатньо реалізована технічно.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

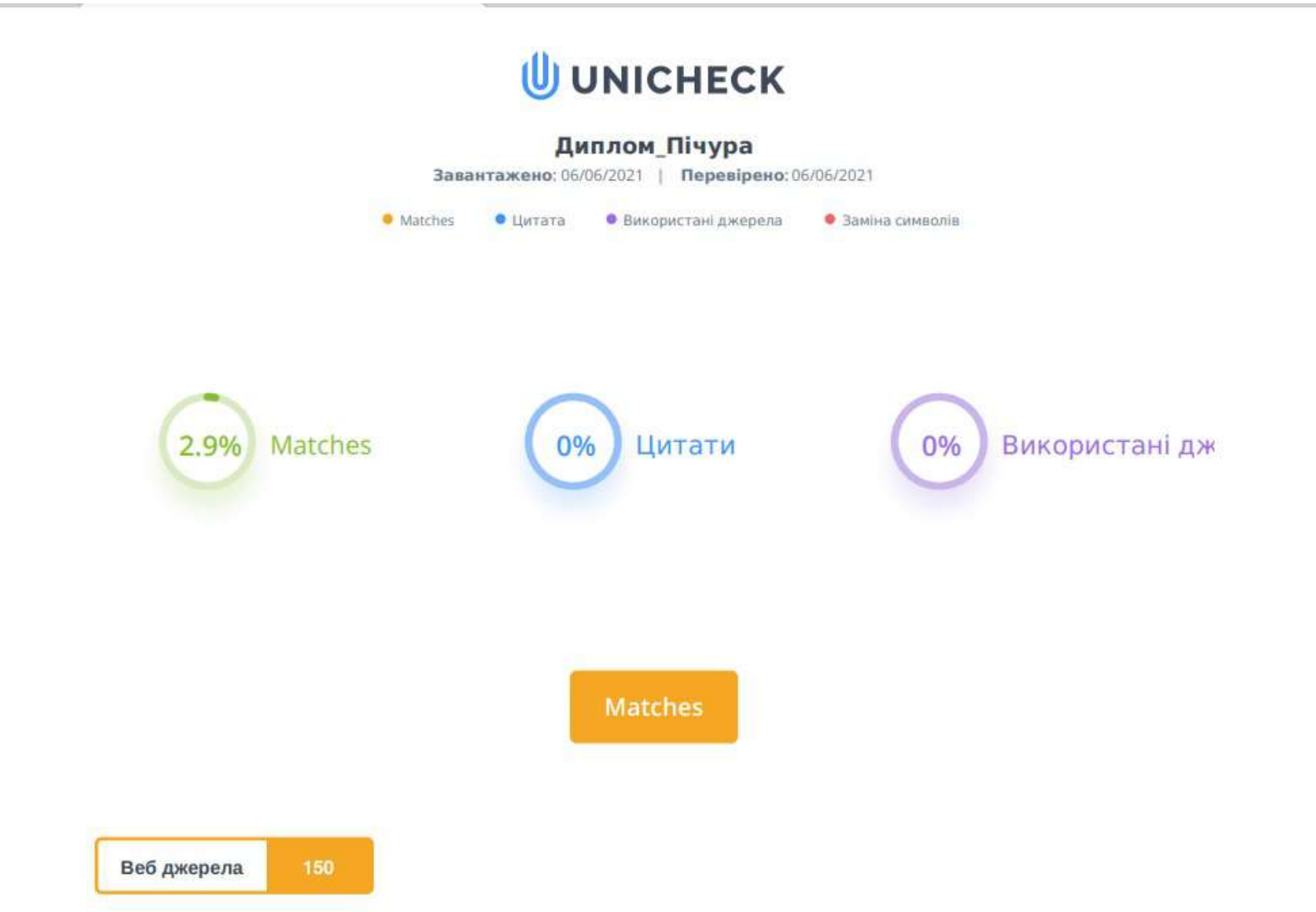
7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує задовільної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Таблиці в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) к.т.н., доцент, доцент каф. КІСТ Кічеворк І.О.

«07» 06 2021. (підпис)


UNICHECK
Диплом_Пічура
Завантажено: 06/06/2021 | Перевірено: 06/06/2021
Matches
Цитата
Використані джерела
Заміна символів
2.9% Matches
0% Цитати
0% Використані дж
Matches
Веб джерела
150

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 8%**

ID: 92428 Название: Система управління інформаційною безпекою в умовах невизначеності та дестабілізуючих факторів Добавлено в БД: 2021-06-07 Авторы: Пічура В.Ю. Руководители: Тітова В.Ю. Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	61236	553	598 (1%)	12 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы