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 магістра

студента Кримчака Павла Вадимовича

академічної групи 125м-21з-1

спеціальності 125 Кібербезпека

за освітньо-професійною програмою Кібербезпека

на тему Розробка моделі управління ризиками інформаційної безпеки в системі електронного документообігу об'єкта критичної інфраструктури

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., професор Корнієнко В.І.			
розділів:				
спеціальний	д.т.н., професор Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викладач Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Кримчаку Павлу Вадимовичу*** **академічної групи** ***125м-21з-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***
(код і назва спеціальності)
за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка моделі управління ризиками інформаційної безпеки в системі електронного документообігу об'єкта критичної інфраструктури***

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

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз проблем інформаційної безпеки в системі електронного документообігу об'єкта критичної інфраструктури	01.11.2022
Розділ 2	Система електронного документообігу. Рекомендації по розробці та впровадженню системи управління ризиками інформаційної безпеки в системі електронного документообігу	30.11.2022
Розділ 3	Визначення та аналіз показників економічної ефективності моделі управління	07.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 17.10.2022р.

Дата подання до екзаменаційної комісії: 09.12.2022р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., __ табл., __ додатків, __ джерел.

Мета магістерської дипломної роботи: забезпечити захист інформації, циркулюючої в системах електронного документообігу шляхом впровадження системи управління ризиками.

Об`єкт дослідження: інформаційна система підрозділів державної інспекції архітектури та містобудування України.

У першій частині проаналізовані існуючі системи електронного документообігу з точки зору інформаційної безпеки та існуючі методи аналізу ризиків. В результаті була обрана модель аналізу ризиків.

У спеціальній частині була розроблена типова модель загроз, проведений аналіз ризиків та запропоновані методи зі зниження ризиків.

У економічній частині виконано розрахунок вартості запропонованих мір з захисту інформації. Надано оцінку економічної ефективності впровадження системи управління ризиками інформаційної безпеки.

В ході роботи розроблені типова модель загроз та приведений приклад впровадження системи управління ризиками державної інспекції архітектури та містобудування України.

ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, МОДЕЛЬ ЗАГРОЗ, АНАЛІЗ РИЗИКІВ, ІНФОРМАЦІЙНИЙ РИЗИК

THE ABSTRACT

The explanatory note: __ pages, __ pictures, __ tables, __additions, __ sources.

The purpose of the work: to ensure of security information, that circulates in the Electronic Document Management System with the help of the embedding of system of risk management.

The object of research: the information system of subdivisions of the State Inspection of Architecture and Urban Planning of Ukraine.

In the first part of our work were analyzed the existing systems of the Electronic Document Management System in the view of information security and existing methods of risk analysis. As a result the proper model of risk analysis was chosen.

In the special part we elaborated the typical model of threats, carried out analysis of risks and suggested the methods of decrease of risks.

In the economical part we calculated the cost of the suggested measures of information security and assessed the economical effectiveness of embedding of the system of risk management.

The work was developed a threat model and an example of implementation of the risk management system of the State Inspection of Architecture and Urban Planning of Ukraine.

INFORMATION SECURITY, RISK MANAGEMENT, MODEL OF THREATS, ANALIS OF RISKS, SNFORMATION RISK

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КС – комп'ютерна система;

НСД – несанкціонований доступ;

ОС – операційна система;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

РК – резервне копіювання;

СЗІ – система захисту інформації;

СУРІБ – система управління ризиками інформаційної безпеки;

УР – управління ризиками;

ДІАМ – державна інспекція архітектури та містобудування України;

К – конфіденційність;

Ц – цілісність;

Д – доступність.

ЗМІСТ

ВСТУП

Найцінніше в будь-якій інформаційно-комунікаційній мережі це інформація, що зберігається в ній, втрата якої може обернутися серйозними неприємностями і навіть фінансовим крахом, як для підприємства в цілому, так і для конкретних користувачів. Відновити інформацію вдається далеко не завжди, до того ж обходиться це недешево, оскільки вимагає спеціальних знань і займає чимало часу.

Інформація має три основних властивості: цілісність, доступність, конфіденційність. З точки зору захисту інформації необхідно приділяти увагу забезпеченню всіх цих властивостей, тому необхідно забезпечити функціонування системи управління ризиками інформаційної безпеки для попередження негативних подій. Тому, не зважаючи на те, що основні зусилля в роботі будуть спрямовані на забезпечення цілісності і доступності, забезпечення конфіденційності також буде розглянуте.

Питанням належного забезпечення інформаційної безпеки інформаційних систем, найчастіше, не надається достатньої уваги. А тим часом вона заслуговує найпильнішої уваги. За найнесприятливішого варіанту розвитку подій втрати можуть бути пов'язані з порушенням конфіденційності інформації, несанкціонованим доступом та витоком інформації.

Від безперебійного функціонування системи електронного документообігу підприємства залежить якість обслуговування споживачів послуг та своєчасний контроль і облік наданих послуг.

Протидія загрозам інформаційній безпеці шляхом контролю ризиків є одним із ключових аспектів успішного функціонування будь-якої сучасної організації. Ризик реалізації певної загрози існує завжди, і ефективність її вирішення буде залежати від того, наскільки підприємство підготовлено до цього.

Один із способів запобігти виникненню несприятливих ситуацій є впровадження системи управління ризиками. Основними проблемами, які можуть виникнути в організації за відсутності такої системи є удар по репутації підприємства, операційні витрати, контрактні порушення, витрати,

пов'язані з «зупинкою і простоєм», зниження прибутку і навіть ліквідація підприємства. Запровадження системи управління ризиками дозволить мінімізувати ризики, що виникають при помилках або відмові обладнання, відмові у системі електроживлення або комунікацій, помилках прикладного програмного забезпечення або пошкодженні баз даних, помилках користувачів, техногенних впливах і природних катаклізмах.

Мета даної роботи полягає в тому, щоб забезпечити рівень безпеки інформації, циркулюючої в системах електронного документообігу шляхом впровадження системи управління ризиками.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз проблеми інформаційної безпеки на рівні надання реєстраційних послуг у сфері будівництва

1.1.1 Характеристика ОІД

Повна назва – Державна інспекція архітектури та містобудування України.

Форма власності – Державна.

Напрям діяльності – надання послуг у сфері будівництва.

Специфіка діяльності підприємства – здійснення в межах повноважень, визначених законом, державного архітектурно-будівельного контролю, архітектурно-будівельного нагляду, ліцензування видів господарської діяльності з будівництва об'єктів, виконання дозвільних та реєстраційних функцій у будівництві.

ОІД – це офісна будівля, яка знаходиться за адресою: 01133, м. Київ, бульвар Лесі Українки, 26.

Розміщення ОІД:

Дислокація:

– схід – пустир 100 метрів;

– південь – оптовий склад на відстані 15 метрів від будівлі;

– північ – 5-ти поверховий житловий будинок на відстані 30 метрів від будівлі;

– захід – одно смугова дорога, котра знаходиться на відстані 20 метрів від будівлі. За дорогою, на відстані 80 метрів від будівлі, розташоване складське приміщення фірми «Євровікна».

До штату співробітників ДІАМ входить 56 осіб.

Таблиця 1.1 – Штат співробітників

Найменування структурного підрозділу	**Найменування посади**	**Кількість штатних одиниць**
Бухгалтерія	Головний бухгалтер	**1**
	Бухгалтер	**3**
Департамент сервісу	Начальник	**1**
	Реєстратори	**37**
Служба on-line підтримки	Спеціаліст	**2**
Керівництво	Голова	**1**
	Заступник голови	**4**
IT - відділ	Інженер-програміст	**2**
	Системний адміністратор	**2**
Фінансова група	Економіст з фінансової роботи	**3**

Категоріювання інформації, що циркулює на ОІД

Згідно НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», категоріюванню підлягають об’єкти, на яких здійснюватиметься обробка технічними засобами та (або) озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці.

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

На даному підприємстві циркулює наступна інформація, що підлягає категоріюванню:

1 Відкрита інформація:

– інформація про послуги, пов`язані з виконанням дозвільних та реєстраційних функцій;

– інформація щодо порядку оплати та умов отримання послуги;

– контактна інформація організації (номера телефонів, адреса, web-сайт);

– організаційно-розпорядча документація (накази, перелік нормативних актів, роз’яснення ДІАМ, постанови КМУ).

2 Конфіденційна інформація:

– договори;

– звіти про надані послуги;

– звіти про здійснення позапланових перевірок;

– звіти про здійснення будівельного нагляду;

– фінансові відомості підприємства;

– журнал обліку вхідних та вихідних документів.

Результати категоріювання наведені в таблиці 1.2.

Рівні наслідків впливу загроз на інформацію з обмеженим доступом:

1 За конфіденційністю (К):

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

Таблиця 1.2 – Категоріювання інформації, що циркулює на ОІД

№	Інформація	Ц	К	Д	Категорія
1	2	3	4	5	6
1	Організаційно-розпоряджувальна інформація	Ц5	К4	Д4	4
2	Журнал обліку внутрішніх документів	Ц5	К5	Д3	4
3	Інформація про послуги підприємства	Ц4	К1	Д4	
4	Інформація про співробітників	Ц5	К5	Д2	4
5	Уставна документація	Ц5	К5	Д3	4
6	Журнал обліку та реєстрації вхідних і вихідних документів	Ц4	К5	Д3	4
7	Трудові договори	Ц5	К2	Д3	4
8	Фінансові відомості підприємства	Ц5	К1	Д2	4
9	Договори, контракти	Ц5	К3	Д3	4
10	Відомості про охоронну сигналізацію	Ц4	К5	Д2	4
11	Звіти про проведені реєстраційні дії	Ц5	К2	Д3	
12	Повна характеристика комп’ютерної та автомобільної техніки	Ц4	К3	Д2	4
13	Звіти про проведення оглядів	Ц4	К1	Д3	
14	Звіти про кількість наданих послуг	Ц4	К2	Д3	

Класифікація інформаційних об'єктів

1 За конфіденційністю:

К5 - критична інформація (розголошення інформації призведе до краху підприємства чи значних матеріальних втрат);

К4 - важлива інформація (розголошення призведе до матеріальних або моральних втрат, якщо не будуть вжиті певні міри);

К3 - значима інформація (приносить моральну шкоду, якщо буде використана в певний момент);

К2 - малозначима інформація (може принести моральну шкоду в дуже рідкісних випадках);

К1 - незначна інформація (не впливає на роботу суб'єкта).

2 За цілісністю:

Ц5 - критична інформація (несанкціонована зміна призведе до неправильної роботи всього підприємства або значної його частини; наслідки такої модифікації незворотні);

Ц4 - дуже важлива інформація (несанкціонована зміна призводить до невірної роботи підприємства або його частини через деякий час, якщо не будуть вжиті певні дії; наслідки такої модифікації незворотні);

Ц3 - важлива інформація (несанкціонована зміна призводить до неправильної роботи підприємства через деякий час, якщо не будуть вжиті певні міри; наслідки такої модифікації оборотні);

Ц2 - значима інформація (несанкціонована зміна позначиться через деякий час, але не призведе до збою в системі; наслідки такої модифікації оборотні);

Ц1 - шкідлива інформація (наявність такої інформації вимагає обробки, а обробка веде до перевитрат ресурсів).

3 За доступністю:

Д5 - критична інформація (робота суб'єкта буде зупинена);

Д4 - важлива інформація (суб'єкт може працювати без цієї інформації деякий час, але вона скоро знадобиться);

Д3 - корисна інформація (без інформації можна працювати, але її використання заощаджує час);

Д2 - неістотна інформація (така інформація, що не впливає на роботу суб'єкта);

Д1 - шкідлива інформація (наявність такої інформації вимагає обробки, а обробка веде до перевитрат ресурсів).

Схема організаційної структури підприємства наведена на рис. 1.1.

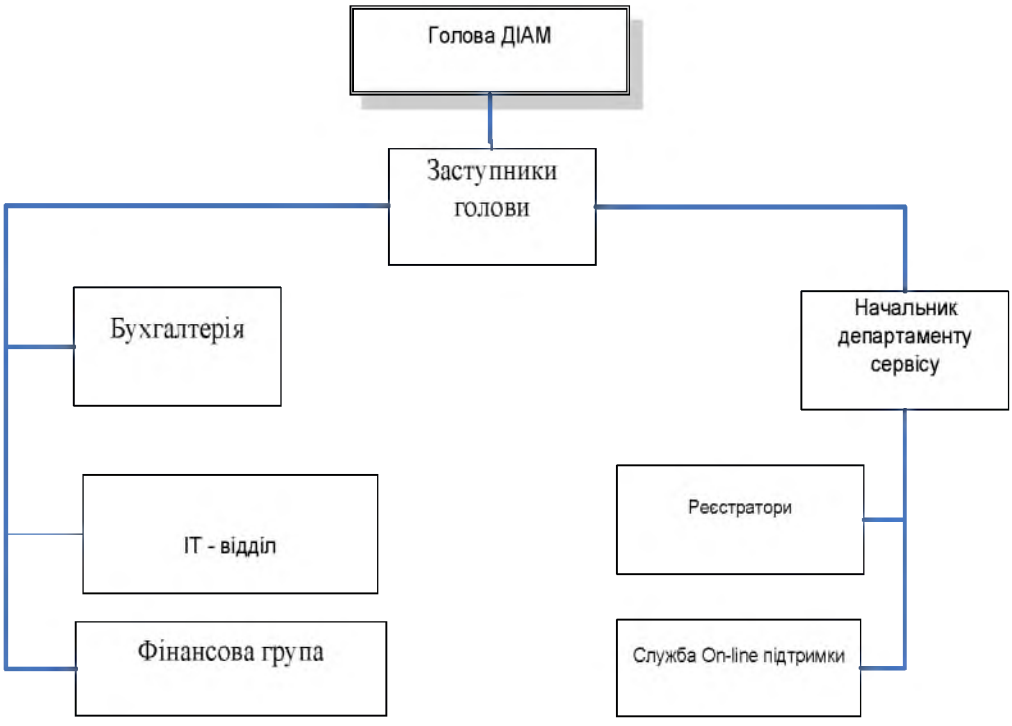

Рис. 1.1 – Організаційна структура ДІАМ

1.1.2 Необхідність захисту інформації на підприємстві

Повноцінне функціонування інформаційних систем спеціального призначення вимагає забезпечення доступності, цілісності, а також конфіденційності оброблюваної у ІС інформації. Порушення безпеки ІС може істотно ускладнити процес оброблення та передавання інформації з обмеженим доступом , тому проблема створення ефективної системи захисту інформації набуває дуже важливого значення.

Питанням належного забезпечення інформаційної безпеки інформаційних систем, найчастіше, не надається достатньої уваги. А тим часом вона заслуговує найпильнішої уваги. За найнесприятливішого варіанту розвитку подій втрати можуть бути пов'язані з порушенням конфіденційності інформації, несанкціонованим доступом та витоком інформації.

Надання реєстраційних послуг підприємством критичної інфраструктури у сфері будівництва – це сприяння надходженню інвестицій та стимулювання економічного розвитку будівельної та супутніх галузей в регіонах та країні в цілому. Надання відповідних послуг суб'єктам господарювання є важливою складовою для запуску будівельного ринку та виробництва будівельних матеріалів, оскільки без отримання відповідних дозволів та ліцензій у суб'єктів містобудування відсутня можливість створювати об'єкти архітектури. ДІАМ проводить свою діяльність у всіх регіонах України через регіональні управління та окремо центральний апарат, який розташований в м. Києві.

З розвитком та впровадженням нових інформаційних та телекомунікаційних технологій зростає і важливість захисту інформації. Інформація стає важливою складовою, яка забезпечує діяльність підприємства. Наслідком цього постає проблема забезпечення інформаційної безпеки. Зі зростанням впливу інформаційних технологій на процес ведення бізнесу, зростають і вимоги до забезпечення захищеності важливої інформації.

1.2 Інформаційна безпека як процес управління ризиками

Згідно НД ТЗІ 1.1-003-99 : Ризик (risk) — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Аналіз ризику (risk analysis) — процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС.

Керування ризиком (risk management) — сукупність заходів, що проводяться протягом всього життєвого циклу АС щодо оцінки ризику, вибору, реалізації і впровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня залишкового ризику.

Залишковий ризик (residual risk) — ризик, що залишається після впровадження заходів забезпечення безпеки.

Система управління ризиками дозволяє отримувати відповіді на наступні питання: - На якому напрямку інформаційної безпеки потрібно зосередити увагу? - Скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації?

Згідно ISO/IEC 27002:2010 вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки. Витрати на контролі повинні бути збалансовані з бізнес-втратами, які можуть бути наслідком порушень безпеки. Результати оцінки ризику допомагатимуть спрямовувати і визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадження контролів, вибраних для захисту від цих ризиків. Оцінка ризиків повинна періодично повторюватися для врахування будь-яких змін, які можуть вплинути на результати оцінки ризику.

1.3 Необхідність ЗІ в системах електронного документообігу

Перед системами електронного документообігу передусім стоять задачі забезпечення цілісності, доступності та конфіденційності інформації, але в силу того, що дані системи набули широкого застосування відносно недавно незважаючи на всі переваги від їх використання ще існує багато проблем забезпечення захищеності даних, які в них обробляються.

Всі системи електронного документообігу мають ті чи інші вбудовані функції безпеки, які загалом засновані на розмежуванні прав доступу в залежності від ролі, яку відіграє користувач системи. Але це не зможе відвернути загрозу несанкціонованого використання конфіденційної інформації авторизованим користувачем. Для забезпечення достовірності документів, що передаються, тобто встановлення авторства відправника, використовують електронний цифровий підпис (ЕЦП), а конфіденційність та цілісність інформації досягається комплексним використанням ЕЦП та шифрування. Як відомо застосування цифрового підпису вимагає використання секретного ключа, яким підписують документ, та відкритого, який дозволяє отримувачу його прочитати. Тому, за умови доступу до комп'ютеру, де зберігається відкритий ключ, у зловмисника виникає можливість влаштувати його підміну і в подальшому видавати себе за авторизованого користувача – отже виникає необхідність захищати не тільки секретні, але й відкриті ключі. Електронний цифровий підпис є єдиним інструментом, який надає юридичної значущості електронним документам, тому розглянута проблема є однією з найбільш важливих.

Захищений документообіг є основою успішного розвитку організації, дозволяє їй використовувати свої фінансові та часові ресурси більш якісно.

1.4 Аналіз системи електронного документообігу

На теперішній час інформаційні системи автоматизації діловодства і документообігу досить широко використовуються в зарубіжній та вітчизняній практиці. Спектр сучасних систем автоматизації діловодства і документообігу досить різноманітний щодо їх функціональності та технологічного рівня.

На даний момент на ОІД встановлена система електронного документообігу «АСКОД». Необхідно проаналізувати захищеність системи електронного документообігу підприємства з точки зору інформаційної безпеки. Результатом даного аналізу буде рішення залишити існуючу систему електронного документообігу або впровадити іншу, яка володіє більшою кількістю позитивних сторін. Для цього дамо характеристику і результати порівняльного аналізу систем, програмних продуктів, які на даний час є лідерами ринку систем автоматизації діловодства і документообігу в Україні.

Для аналізу розглянемо продукти:

1) Almexoft;
2) 1С Документообіг;
3) ДОКПРОФ;
4) АСКОД;
5) ЕВФАРТ.

1.4.1 Almexoft (https://almexoft.com)

Платформа Almexoft побудована за принципом low-code, що дає можливість налаштування різних бізнес-процесів без програмування і перекомпіляції ядра системи. Для реалізації обраної парадигми роботи в системі реалізований візуальний редактор бізнес-процесів і форм даних, де бізнес-процеси представляються у вигляді етапів обробки примірника процесу і зв'язків між ними. Нотація конструктора близька до загальноприйнятої BPMN 2.0, але для зручності побудови деякі атрибути бізнес-процесу збільшені, винесені у

властивості. Зручний редактор властивостей процесу (object inspector) дозволяє швидко кастомізувати обраний об'єкт (етап, перехід). Широкі можливості налаштування кожного об'єкта дозволяють управляти термінами виконання етапу, умовами переходу, доступністю дій для користувача, повідомленнями, правилами роботи з вкладеннями, видимістю полів, вкладень, вкладок.

Платформа пропонує широкий набір стандартних елементів для побудови бізнес-процесів, і, одночасно, дозволяє додавати елементи, створені сторонніми розробниками. Платформа дозволяє виділяти часто використовувані конструкції в окремі підпроцеси для перевикористання в рамках інших бізнес-процесів. Додатково є можливість будувати зв'язки між процесами з можливістю передачі полів картки процесу. Редактор має вбудовані механізми валідації, що дозволяє точно ідентифікувати місце виникнення проблеми при побудові бізнес-процесу та оперативно усунути їх без залучення фахівців вендоравлади та ін.

1.4.2 1С Документообіг(http://1c.ru/)

"1С: Документообіг" дозволяє:

- впорядкувати роботу співробітників з документами, виключити можливість втрати версій або перетину фрагментів при одночасній роботі;
- скоротити час пошуку потрібної інформації і сумарний час колективної обробки документів;
- підвищити якість готового матеріалу (проектів, документації тощо) за рахунок вирішення великої кількості спірних питань та впорядкування роботи користувачів.

"1С: Документообіг" не має галузевої специфіки і може ефективно використовуватися як в бюджетному секторі, так і на комерційних підприємствах, будь то розподілена холдингова структура з великою кількістю користувачів або невелике підприємство. Будучи універсальною, програма

легко може бути налаштована і адаптована під специфіку конкретної організації.

"1С: Документообіг" у комплексі вирішує завдання автоматизації обліку документів, взаємодії співробітників, контролю та аналізу виконавської дисципліни:

- централізоване безпечне зберігання документів,
- оперативний доступ до документів з урахуванням прав користувачів,
- реєстрація вхідних і вихідних документів,
- перегляд і редагування документів,
- контроль версій документів,
- робота з документами будь-яких типів: офісними документами, текстами, зображеннями, аудіо-та відеофайлами, документами систем проектування, архівами, додатками і т.д.,
- повнотекстовий пошук документів за їх змістом,
- колективна робота користувачів з можливістю узгодження, затвердження та контролю виконання документів,
- маршрутизація документів, що настроюється по кожному виду документів окремо,
- автоматизована завантаження документів з електронної пошти і зі сканера,
- облік і контроль робочого часу співробітників.

Облік документів ведеться в розрізі видів документів відповідно до положення про документообіг підприємства. Принципи обліку вхідних, вихідних і внутрішніх документів, закладені в програму, повністю відповідають діючим стандартам і нормам, наприклад:

- ГОСТ Р 6.30-2003,
- ГОСТ Р 51141-98,
- Федеральний закон Російської Федерації від 27.07.2006 р. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

- Вимоги ГСДОУ,
- Типова інструкція з діловодства в органах федеральної виконавчої влади та ін.

1.4.3 ДОКПРОФ (https://www.docprof.ua)

Користувачами системи електронного документообігу ДОКПРОФ є органи державної влади, державні унітарні підприємства, комерційні компанії, серед яких як холдинги з великою філіальною структурою, так і невеликі організації.

Автоматизація управління документами за допомогою ДОКПРОФ призводить до зростання продуктивності роботи працівників, полегшення доступу до інформації для прийняття управлінських рішень, поліпшенню виконавської дисципліни, і, отже, до загального підвищення якості управління.

Ядро Системи побудовано за принципами 2-рівневої клієнт-серверної архітектури та забезпечує високу доступність Системи, низьку латентність при обробці запитів, зниження вимог до технічного забезпечення серверної компоненти за рахунок перерозподілу навантаження між сервером та робочими станціями клієнтів.

Сховище даних Системи побудоване у вигляді централізованої бази даних (централізована архітектура). Система надає можливість використання оперативного та довгострокового архівів (розподілена мультисерверна архітектура). При використанні розподіленої архітектури історичні та архівні дані можуть бути винесені на окремі сховища даних зі зниженими вимогами до швидкості доступу. Доступ до актуальних та архівних даних в Системі відбувається прозоро для користувача та не потребує явного переключення між основними та архівними серверами.

Клієнтське робоче місце ДОКПРОФ є універсальним, тобто має набір функцій і модулів, що використовуються, регламентується тільки повноваженнями та правами користувача і не вимагає установки додаткового програмного забезпечення. Для забезпечення інтеграції з порталами послуг та

іншими зовнішніми сервісами використовується власна модульна шина веб-сервісів (на основі серверу застосувань Apache TomCat, протоколів soap та rest, технології Java).Є можливість комфортної роботи географічно-віддалених користувачів за умови мінімальної швидкості передачі даних каналами зв'язку (до 128 Кбіт/сек) чи за її короткочасної відсутності. Є можливість авторизації та ідентифікації користувачів СЕД, у тому числі з використанням засобів ЕЦП, Active Directory, логінів та паролів.

1.4.4АСКОД(https://askod.ua)

Система електронного документообігу АСКОД здійснює ефективне управління корпоративними інформаційними ресурсами, що дозволяє швидко і прозоро організувати та автоматизувати управлінські бізнес-процеси як в умовах централізованої, так і територіально-розподіленої організаційної структури.

Система АСКОД у хмарі - сучасний інструмент обслуговування клієнтів, що полягає у наданні доступу до функціональності системи АСКОД.

Організація електронного документообігу АСКОД у хмарі дозволить заощадити фінансові ресурси клієнта за рахунок відсутності витрат на інсталяцію програмного забезпечення, його періодичного оновлення, а також технічного обслуговування апаратних засобів, необхідних для роботи системи електронного документообігу.

Хмара розгорнута на високотехнологічному майданчику DataStore, що розташований в столиці України та має рівень резервування всіх інженерних та IT систем за формулою N+1 і відповідає вимогам міжнародних стандартів TIA - 942 у класі TIER3.

Програмне забезпечення системи електронного документообігу АСКОД, має чинний експертний висновок, зареєстрований в Держспецзв'язку України, який засвідчує рівень Г-3 гарантій реалізації функціонального профілю безпеки.

Система АСКОД у хмарі забезпечує постійну доступність до всіх сервісів у режимі 24х7, крім випадків, коли в системі електронного документообігу виконуються планові профілактичні роботи або відбувається оновлення програмного забезпечення, про що користувачі інформуються заздалегідь.

Під час використання системи АСКОД у хмарі АСКОД на сервері виконується постійне резервне копіювання даних для їх збереження.

Додаткові можливості та послуги системи:

• розробка додаткових модулів до системи, відповідно до вимог замовника;

• навчання користувачів та адміністраторів;

• розробка програмного забезпечення;

• інтеграція з іншими інформаційними системами;

• розробка технічної та проєктної документації.

1.4.5ЕВФАРТ(http://www.evfrat.ru/)

Система «Евфрат» забезпечує весь життєвий цикл електронних документів у рамках ключових бізнес-процесів організації:

Введення і реєстрація документів. Паперові та електронні документи можуть бути автоматично імпортовані в систему. Механізм «розуміння» документів (пошук в електронному документі реквізитів і даних) і технологія Drag & Recog (розпізнавання реквізитів з відсканованого документа) забезпечують максимальну автоматизацію введення і реєстрації документів в системі.

Робота з електронними документами. Застосовувана схема документообігу забезпечує зберігання документів усіх типів в єдиній базі і надає такі можливості, як пакетний введення паперових документів, автоімпорт та підтримка версійності документів, повнотекстовий пошук, створення аналітичних звітів і багато іншого.

Контроль виконання. Взаємодія співробітників в ході бізнес-процесів підтримується системою погоджень і доручень, гарантовано підвищує

виконавську дисципліну. Важливий документ не загубиться в ході узгоджень. Завжди є можливість відстежити, на якій стадії роботи він знаходиться. Час узгодження документів скорочується в рази.

Оптимізація руху документів (технологія Workflow). Реальні бізнес-процеси компанії підтримуються за рахунок використання концепцій WorkFlow і BPM. У візуальному редакторі можна створювати жорсткі й гнучкі маршрути будь-якої складності, де блоки схеми та зв'язку представлені в наочній графічній формі. Автоматично виконуються найбільш стандартизовані операції: реєстрація документів, приєднання файлів, запуск документів за типовими маршрутами, створення зв'язків між документами, формування типових документів та підготовка відповідей на запити за шаблонами.

Розсилка документів. Автоматична розсилка документів за адресами електронної пошти дозволяє позбутися від рутинних процесів, на які витрачається значна частина робочого часу. Ви можете налаштувати повідомлення на всі можливі випадки для різних типів користувачів.

Зберігання документів. Система дозволяє створити єдиний електронний архів документів практично необмеженого обсягу і ефективно управляти ним. Підтримка версійності дозволяє вести всю історію змін документа, не загубивши ані найменшої деталі. Завдяки засобам оперативного пошуку ви зможете знайти потрібний документ за секунди, а система автоматичного резервного копіювання дозволить надійно зберігати базу документів.

Внутрішня пошта. Система дозволяє здійснювати внутрішню переписку між співробітниками з використанням вбудованого поштового клієнта, який володіє усіма функціями стандартних поштовиків. Таким чином, користувачі можуть обмінюватися всіма типами інформації в рамках єдиної системи.

1.4.6Результати аналізу систем електронного документообігу

Результати порівняльного аналізу систем електронного документообігу приведені в таблиці 1.3 «Порівняльна характеристика СЕД».

Як ми бачимо з результатів аналізу, немає необхідності в заміні встановленої СЕД «АСКОД», оскільки вона володіє достатнім рівнем вбудованої захищеності.

Таблиця 1.3 «Порівняльна характеристика СЕД»

Критерій	Almexsoft	1С Документооборот	ДОКПРОФ	АСКОД	ЕВФАРТ
Програмні засоби контролю цілісності документів	+	-	+	+	+
Динамічне блокування документу	+	+	+	+	+
Засоби моніторингу подій	+	+	+	+	+
Видача прав на тимчасове користування	-	-	+	+	-
Ведення протоколу дій користувача	+	+	+	+	+
Розмежування прав на рівні РКК	-	-	+	+	+
Накладання резолюцій	+	-	-	+	+
Права, ролі	-	+	+	+	+
Криптографія, ЕЦП	+	+	+	+	+
Резервне копіювання	+	+	+	+	+
Загальна оцінка	7	6	10	10	9

1.5 Аналіз методів управління ризиками

Управління ризиками ІБ підприємства потребує:

- ідентифікацію ризиків;
- визначення розміру ризику;
- розробка плану управління ризиками;
- поточний контроль і управління ризиками.

Згідно ISO/IEC 27002:2010: під час оцінювання ризику ідентифікують загрози активам і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу.

Оцінка ризиків повинна містити системний підхід до визначення кількісно оціненого ризику (аналізування ризику) та процес порівняння кількісно оцінених ризиків з критеріями ризику для встановлення його значимості (визначення ризику).

Оцінки ризиків повинні також проводитись періодично для урахування змін у вимогах безпеки і ситуації з ризиками, наприклад, щодо активів, загроз, вразливостей, значних впливів, оцінювання ризику, а також коли відбуваються значні зміни. Ці оцінки ризиків треба здійснювати системним способом, який надає можливість отримати порівнювані та відтворювані результати.

Рис. 1.2 – Залежність процесів, пов'язаних з управлінням ризиками в області ІБ

Для встановлення моделі управління ризиками проаналізуємо існуючі моделі.

1.5.1 Модель якісної оцінки «Ризик атаки – Важливість активу»

Модель якісної оцінки ризики зводиться до побудови таблиці 1.4.

Таблиця заповнюється екземплярами інформаційних активів або окремими системами на основі інтуїтивного уявлення заповнюю чого про ту чи іншу інформацію, або на основі заповнення підготовлених анкет для компетентних співробітників організації. Рішення приймається в залежності від конкретної організації для об'єктів, що знаходяться у третій зоні або у третій та другій зонах.

Таблиця 1.4 – «Ризик атаки – Важливість активу»

	Важливий	Критичний	Життєвий
Низький	1	1	2
Середній	1	2	3
Високий	2	3	3

Можливий ще більш спрощений підхід, який називається «основна лінія», який полягає у тому, що організація аналізує стан побудови систем безпеки, який склався в галузі(можливо в організаціях, схожих за профілем), та порівнює з системою безпеки, побудованої в самій компанії. Якщо виявиться відставання, ресурси направляються на приведення ситуації до рівня, близькому до середнього в галузі.

Позитивні сторони оцінки ризику по якісній моделі полягають у наступному:

- розрахунки прискорюються та спрощуються;
- немає необхідності привласнювати грошову вартість активу;
- немає необхідності обчислювати частоту появи загрози та точний розмір збитків;
- не потрібно обчислювати відповідність ефективності запропонованих мір загрозам.

Негативні сторони полягають в основному в суб'єктивності підходу до оцінки та відсутності можливості встановити точну відповідність затрат загрозам.

1.5.2 Модель якісної оцінки ризику на основі побудови матриці «Вірогідність - втрати»

Для визначення ступеня впливу та рівня ризику використовують наступні градації: високий, середній, низький. Проте на практиці важливо визначити ступінь впливу кожного ризику відносному вираженні, для чого рекомендують використовувати шкалу від 1 до 5 (Таблиця 1.5).

Таблиця 1.5 Ступінь впливу ризику

Матриця «Вірогідність - Втрати»		**Втрати**				
		1	**2**	**3**	**4**	**5**
Вірогідність	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Ймовірність виникнення:

1) слабкоймовірні;
2) малоймовірні;
3) ймовірні;
4) досить ймовірні;
5) майже можливі.

Величина втрат:

1) мінімальні;
2) низькі;
3) середні;
4) високі;
5) максимальні.

Ступінь впливу:

1) ігноровані(1-4);
2) незначні(5-8);
3) помірні(9-10);
4) суттєві(12-16);
5) критичні(20-25).

Рівень ризику:

1) прийнятні(1-4);
2) виправдані(5-11);
3) неприпустимі(12-25).

1.5.3 Кількісна модель оцінки ризиків «Очікуваний річний збиток»

Кількісна модель ризиків оперує такими поняттями, як:

- річна частота події (англ. Annualized Rate of OccurrenceARO);
- очікуваний одиничний збиток (англ. Single Loss Expectancy - SLE);
- очікуваний річний збиток (англ. Annualized Loss Expectancy - ALE), величина, що дорівнює добутку ARO на SLE.

ALE = ARO 'SLE ,

де ARO - частота появи події, що приносить шкоду на рік. Даний показник також можна назвати інтенсивністю події. SLE - показник, який розраховується як добуток вартості інформації (Asset Value - AV) на фактор впливу

(англ.Exposure Factor - EF). Фактор впливу - це розмір збитку або впливу на значення активу (від 0 до 1), тобто частина значення, яку актив втратить в результаті події.

SLE = AV 'EF.

Управління ризиками вважається ефективним, якщо витрати на безпека на рік не перевищують очікуваний річний збиток. Приклад. Мається підприємство з внутрішньою інфраструктурою загальною вартістю 200 000 дол. Пожежа може завдати шкоди з фактором впливу 0,3. Пожежа може трапитися раз на 10 років. Тоді:

SLE = 200000 '0,3 = 60000,

ALE = 60000 '0,1 = 6000.

Таким чином, якщо підприємство витрачає до 6000 дол. на рік, то управління ризиками здійснюється вірно.

1.5.4 Модель узагальненого вартісного результату Міори(GCC)

Модель Міори розроблена як альтернатива кількісної моделі ризиків для поліпшення і полегшення розрахунків і обчислень. Одним з основних недоліків якої є її імовірнісна складова.

Модель Міори не враховує ймовірностей події, вона оперує поняттям збитку від простою як функцією часу після настання події. Для кожного інформаційного активу або групи подібних по ряду ознак активів, званих категорією, визначається розмір можливого збитку, термін початку його впливу на організацію та розподіленість за часом.

Розвиток картини збитку можна представити у вигляді графіка, де категорії - це функції по двох осях: «час у днях»; «збиток в грошах». У результуючому графіку представляються дві криві: сумарний збиток організації за відсутності захисних заходів; сумарний збиток прі наявності захисних заходів.

На такому графіку наочно видно необхідність і ефективність застосовуваних заходів для забезпечення захисту інформації.

1.5.5 Модель оцінки ризику за двома факторами

В таблиці можна наглядно відобразити зв'язок факторів негативного впливу(показників ресурсів) та ймовірностей реалізації загрози з урахуванням показників вразливостей.

На першому кроці оцінюється негативний вплив(показник ресурсу) по заздалегідь визначеній шкалі, наприклад від 1 до 5, для кожного ресурсу,якому загрожує небезпека(колонка b в таблиці).

На першому кроці оцінюється по заздалегідь визначеній шкалі, наприклад від 1 до 5, визначається вірогідність реалізації кожної загрози.

На третьому кроці обчислюється показник ризику. В найпростішому варіанті методики це робиться шляхом множення(b, x, c). Проте необхідно розуміти, що операція множення визначена для кількісних шкал. Для рангових(якісних) шкал вимірювання, якими являються показник негативного впливу та ймовірність реалізації загрози, наприклад, зовсім не обов'язково показник ризику, відповідних ситуації b=3, c=1 буде еквівалентний b=1, c=3. Відповідно, повинна бути розроблена методика оцінки показників ризику стосовно конкретної організації.

На четвертому кроці загрози ранжуються за значенням їхнього фактора ризику(Таблиця 1.6).

Таблиця 1.6 – Ранжування ризиків

Дескриптор загрози	Показник негативного впливу(ресурса)	Можливість реалізації загрози (суб’єктивна оцінка)	Показник ризику	Ранг ризику
Загроза А	5	2	10	2

Загроза B	2	4	8	3
Загроза C	3	5	15	1

Дана процедура дозволяє порівняти та ранжувати загрози з різним негативним впливом та ймовірністю реалізації. В деяких випадках додатково можуть прийматись до уваги вартісні показники.

1.5.6 Модель оцінки ризику за трьома факторами

По кожній групі ресурсів, пов'язаних з даною загрозою, оцінюються рівень загрози(ймовірність реалізації) та рівень вразливості(ступінь легкості, з якою реалізована загроза здатна привести до негативного впливу). Оцінювання проводиться в якісних шкалах.

Спочатку визначають рівні загроз, вразливостей, тяжкості наслідків і ризиків:

Рівні загроз:

Низький(H) – реалізація даної загрози маловірогідна, за останні 2 роки подібних випадків не зафіксовано.

Середній(C) – загроза може бути реалізована протягом 1 року з вірогідністю приблизно 0.3.

Високий(B) – загроза більш за все реалізується протягом року і можливо не один раз.

Рівні вразливостей:

Низький(H) – захищеність системи дуже висока, реалізація загроз майже ніколи не призводить до негативних наслідків.

Середній(C) – захищеність системи середня, реалізація приблизно 30% загроз призводить до негативних наслідків.

Високий(В) – захищеність системи дуже низька, реалізація загроз майже завжди призводить до негативних наслідків.

Показники негативного впливу(тяжкості наслідків):

1) Negligible (до $100)
2) Minor (до $1000)
3) Moderate (до $10000)
4) Serious (Суттєвий негативний вплив на бізнес)
5) Critical (Катастрофічний вплив, можлива зупинка)

Рівні ризиків:

Показник ризику вимірюється в шкалі від 0 до 8, визначення рівнів ризику представлене в таблиці 1.7.

Таблиця 1.7 – Ступінь серйозності випадків

Ступінь серйозності випадку (ціна втрати)	Рівень загрози								
	Низький			Середній			Високий		
	Рівень вразливості			Рівень вразливості			Рівень вразливості		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

1.5.7 Результати оцінки методів аналізу ризиків

Для вибору методики управління ризику проаналізовано описані методи, щоб обрати ті, які найбільш підходять. Критерії обрані на основі простоти впровадження, точності та наглядності оцінки ризиків. Результати аналізу приведені в таблиці 1.8 «Оцінка методів аналізу ризиків».

З результатів аналізу можна зробити висновки, що біль доцільно використати модель оцінки ризиків «Очікуваний річний збиток». На основі

даної моделі необхідно створювати модель управління ризиками для даного ОІД.

Таблиця 1.8 Оцінка методів аналізу ризиків

Критерій	Ризик атаки – Важливість активу	Вірогідність - Втрати	Очікуваний річний збиток	GCC	за двома факторами	за трьома факторами
Простота в оцінці ризику	+	+	+	+	+	-
Незалежність результатів від суб'єктивної думки	-	-	+	-	-	-
Достатня різниця між існуючими ризиками	-	+	+	-	-	+
Точність оцінювання	-	-	+-	+	-	-
Незалежність від кваліфікації створеної групи	-	-	+	-	-	-
Наглядність у визначенні розміру інвестицій	+	-	+	+	+	+
Необхідність глибоких знань у даній сфері	+	+	+	+	+	+
Загальна оцінка	3	3	6,5	4	3	4

В першу чергу необхідно встановити критерії прийняття ризику та класифікувати ризики в залежності від величини можливих втрат для конкретного підприємства. Для оцінки ризиків більш доцільно використати кількісні методи оцінки, оскільки якісні не характеризують ризики так точно як кількісні. Для адекватного вибору критеріїв оцінки ризиків необхідно спочатку визначити вартість активів. Це пояснюється тим, що встановивши критерії ризику без урахування їх вартості, всі ризики можуть потрапити в одну категорію, що буде не правильним. Тобто спочатку необхідно визначити вартість активів.

На наступному кроці необхідно визначити фактори, від яких залежить ступінь ризику та оцінити вірогідність виникнення кожного ризику. Ресурс повинен бути проаналізований з точки зору оцінки впливу можливих атак та

небажаних подій природного походження. Крім того необхідно ідентифікувати вразливості, які роблять можливою реалізацію загрози. Тобто необхідно створити модель загроз та на її основі визначити рівень ризику. Для цього послідовно для кожної загрози необхідно визначити:

- найменування загрози;
- об'єкт загрози;
- використані вразливості;
- вплив на властивості інформації;
- можливі наслідки.

Також необхідно брати до уваги той факт що деякі ризики можуть виникати частіше, деякі рідше, тому для адекватної оцінки необхідно аналізувати ймовірність виникнення та вірогідні втрати як один показник. Оцінити ризик можна за допомогою таблиці. Результатом оцінки будуть показники очікуваний річний збиток та пріоритет ризику(Таблиця 1.9).

Таблиця 1.9 – Оцінка ризиків

Загроза	Річна частота події	Очікуваний одиничний збиток	Очікуваний річний збиток	Пріоритет ризику
Загроза 1	P1	S1	P1xS1	R1
Загроза 2	P2	S2	P2xS2	R2
Загроза 3	P3	S3	P3xS3	R3

Після проведення аналізу ризиків необхідно встановити міри зі зниження ризиків та оцінити рівень ризику після прийняття мір. Оскільки переоцінка активів проводиться раз на рік, то доцільно проводити переоцінку ризиків також раз на рік.

1.6 Висновок. Постановка задачі

Мета даної магістерської дипломної роботи: забезпечити рівень безпеки інформації, циркулюючої в системах електронного документообігу шляхом впровадження системи управління ризиками.

Завдання роботи:

- аналіз загроз ІБ в СЕД;
- оцінити вразливість та ймовірність подій і визначити величину потенційного впливу для кожної загрози;
- встановлення моделі управління ризиками;
- розробка рекомендацій зі зменшення ризиків, що застосовуються до ІС будь-якого регіонального підрозділу компанії.

Об'єкт дослідження: інформаційна система підрозділів ДІАМ.

Предмет дослідження: моделі управління ризиками та системи електронного документообігу з точки зору ІБ.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Система електронного документообігу

2.1.1 Принципи організації роботи систем електронного документообігу

Основні принципи організації електронного документообігу:

- Одноразова реєстрація документа
- Можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання
- Безперервність руху документа
- Єдина база документованої інформації для централізованого зберігання документів і виключення можливості дублювання документів
- Ефективно організована система пошуку документа
- Розвинена система звітності, що дозволяє контролювати рух документа в процесі документообігу.

2.1.2 Функції систем електронного документообігу

У відповідності з основними принципами організації електронного документообігу СЕД забезпечують виконання таких функцій:

Централізоване управління документами – СЕД дозволяють оперативно змінювати форми документів, що використовуються в організації.

Підтримка життєвого циклу документів – СЕД дозволяють жорстко контролювати життєвий цикл документів з урахуванням вимог корпоративного середовища, а також галузевих стандартів і законодавства.

Колективна робота над документами – СЕД дозволяють організувати колективну роботу над документом; причому в ній можуть брати участь фахівці, що знаходяться в різних офісах.

Забезпечення конфіденційності – СЕД забезпечують можливість підписувати документи за допомогою електронного підпису і зашифровувати їх.

Маршрутизація документів – СЕД забезпечують автоматичну передачу документу потрібній особі.

Інтеграція з іншими системами – СЕД, як правило, повинні і можуть бути інтегровані з іншими системами управління підприємством - бухгалтерськими, виробничими, фінансовими, аналітичними і т.д.

Управління доступом – СЕД дозволяють розмежувати повноваження співробітників організації і здійснювати контроль за доступом до документів.

2.1.3 Система «АСКОД»

Система електронного документообігу АСКОД https://askod.ua здійснює ефективне управління корпоративними інформаційними ресурсами, що дозволяє швидко і прозоро організувати та автоматизувати управлінські бізнес-процеси як в умовах централізованої, так і територіально-розподіленої організаційної структури.

Система АСКОД у хмарі - сучасний інструмент обслуговування клієнтів, що полягає у наданні доступу до функціональності системи АСКОД.

Організація електронного документообігу АСКОД у хмарі дозволить заощадити фінансові ресурси клієнта за рахунок відсутності витрат на інсталяцію програмного забезпечення, його періодичного оновлення, а також технічного обслуговування апаратних засобів, необхідних для роботи системи електронного документообігу.

Хмара розгорнута на високотехнологічному майданчику DataStore, що розташований в столиці України та має рівень резервування всіх інженерних та IT систем за формулою N+1 і відповідає вимогам міжнародних стандартів TIA - 942 у класі TIER3.

Програмне забезпечення системи електронного документообігу АСКОД, має чинний експертний висновок, зареєстрований в Держспецзв'язку України, який засвідчує рівень Г-3 гарантій реалізації функціонального профілю безпеки.

Система АСКОД у хмарі забезпечує постійну доступність до всіх сервісів у режимі 24х7, крім випадків, коли в системі електронного документообігу виконуються планові профілактичні роботи або відбувається оновлення програмного забезпечення, про що користувачі інформуються заздалегідь.

Під час використання системи АСКОД у хмарі АСКОД на сервері виконується постійне резервне копіювання даних для їх збереження.

Додаткові можливості та послуги системи:

• розробка додаткових модулів до системи, відповідно до вимог замовника;

• навчання користувачів та адміністраторів;

• розробка програмного забезпечення;

• інтеграція з іншими інформаційними системами;

• розробка технічної та проєктної документації.

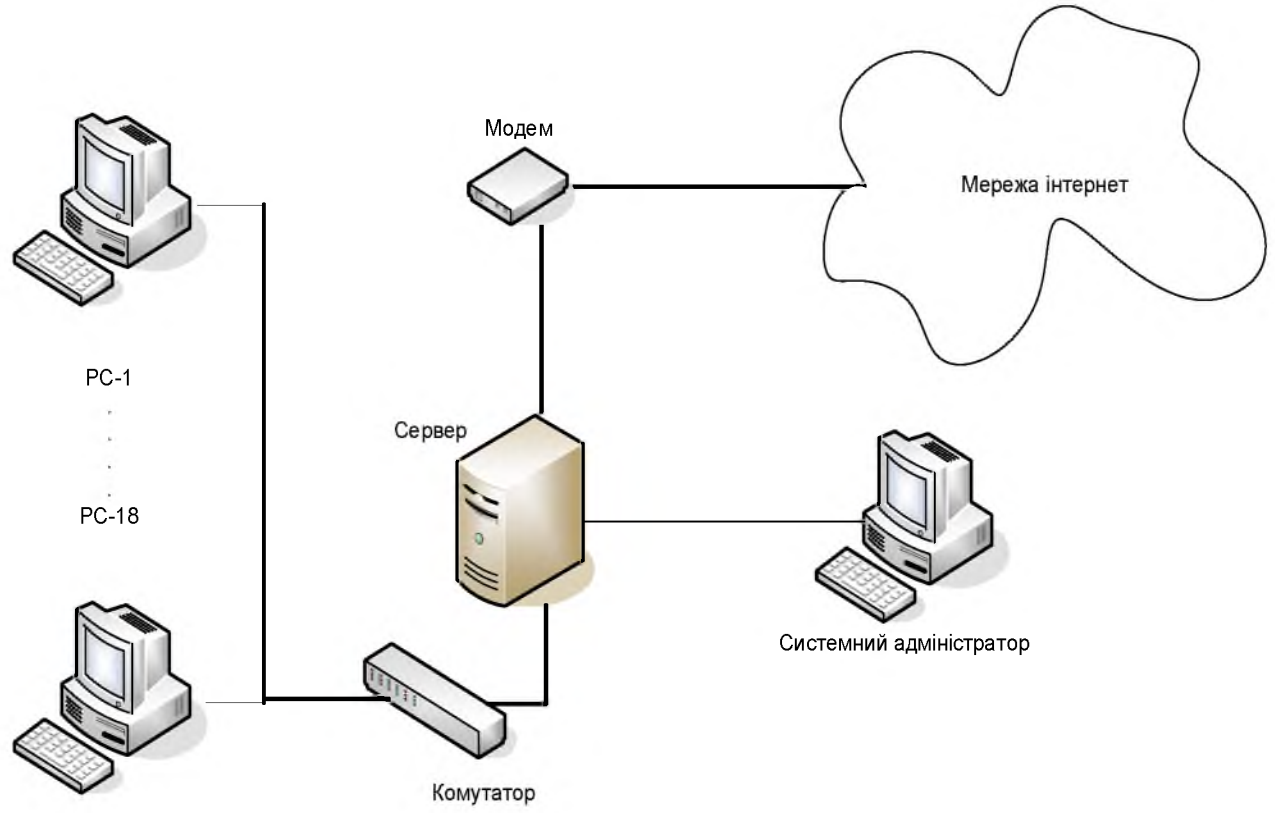

Рис 2.1 Схема комп'ютерної мережі

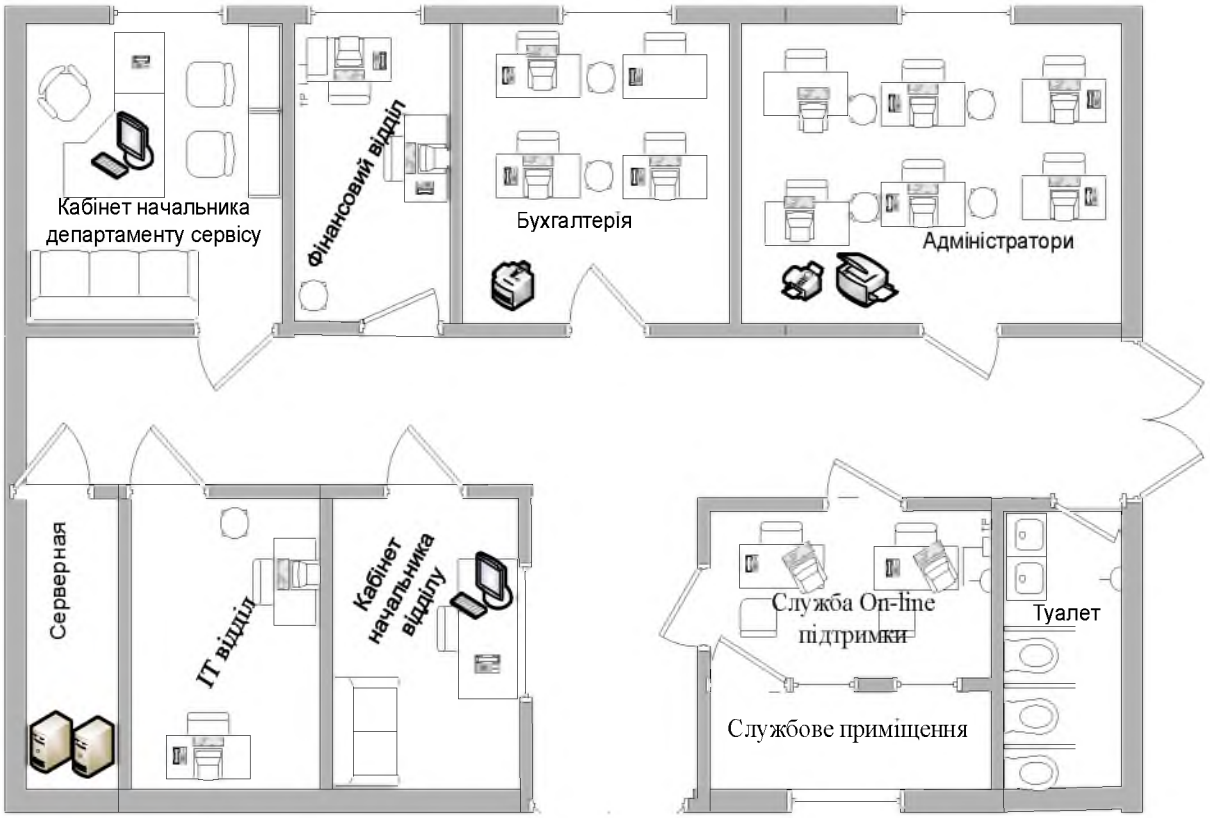

Рис 2.2 Генеральний план підприємства

В таблиці 2.1 відображено, до якої інформації які співробітники мають доступ. Номер інформації згідно таблиці 1.2.

Таблиця 2.1 – Права доступу до інформації

Найменування посади	**Кількість штатних одиниць**
Головний бухгалтер	**1, 3, 4, 5, 8, 9, 11, 14**
Бухгалтер	**1, 3, 5, 8, 9, 11, 14**
Адміністратори	**1, 3, 5, 11, 13, 14**
Служба On-line підтримки	**1, 3, 5, 11, 13, 14**
Начальник управління	**1 – 14**
Начальник департаменту сервісу	**1 – 14**
IT - спеціаліст	**6, 10**
Системний адміністратор	**6, 2, 12, 4, 7, 10**
Економіст	**1, 3, 5, 8, 9, 11, 14**

2.2 Рекомендації до впровадження СУРІБ для систем електронного документообігу ДІАМ.

2.2.1 Оцінка вартості активів

Процес управління ризиками розпочинається з оцінки активів. Вартість активів встановлює власник інформації. Необхідно проводити переоцінку один раз на рік.

2.2.2 Оцінка ризику

Оцінку ризику необхідно проводити за факторами, які впливають на ризики. Тобто для кожної загрози необхідно визначити:

- найменування загрози;
- об’єкт загрози;
- вразливості;
- вплив на властивості інформації;
- можливі наслідки.

2.2.2 Встановлення критерії прийняття ризиків

Необхідно встановити критерії прийняття ризиків виходячи з інформації про вартість активів. На цьому кроці визначаються ризики, які можна прийняти, та ризики, рівень яких необхідно знижувати в першу чергу. Для встановлення критеріїв прийняття ризику необхідно для трьох категорій визначити кількісні варіації ризику.

Таблиця 2.2 – Критерії прийняття ризику

Пріоритет ризику	Ступінь впливу, грн
1 - Високий	від 3000
2- Середній	500-3000
3- Прийнятний	до 500

2.2.3 Визначення пріоритетів ризику

На даному етапі необхідно встановити річну частоту події, очікуваний одиничний збиток, ступінь впливу та визначити очікуваний річний збиток. На

основі даної оцінки визначити пріоритет для кожного ризику. Тобто необхідно заповнити таблицю 2.8.

Таблиця 2.3 – Пріоритет ризику

Загроза	Річна частота події	Очікуваний одиничний збиток	Ступінь впливу	Очікуваний річний збиток	Пріоритет ризику
Загроза 1	P1	S1	V1	P1xS1xV1	R1
Загроза 2	P2	S2	V2	P2xS2xV2	R2
Загроза 3	P3	S3	V3	P3xS3xV3	R3

2.2.4 Визначення контрмір

Для кожного ризику визначають міри зі зниження. Далі визначаються міри, які необхідно запровадити в першу чергу. Проводиться оцінка ефективності запропонованих мір за результатами впливу на рівень ризику.

Таблиця 2.4 – Визначення мір зі зниження ризику

Загроза	Рівень ризику	Міри зі зниження ризику	Пріоритет ризику
Найменування	розмір втрат	перелік	1 – 3

Пріритетними повинні бути контрміри, які впливать на ризики з високим рівнем. Далі проводиться більш детальна характеристика мір та їх вартість.

Таблиця 2.5 – Характеристика мір зі зниження ризику

Міри	Характеристика	Вартість
найменування	опис (найменування)	грн

2.2.5 Журнал опису ризиків

В журнал опису ризиків вноситься вся інформаці, яка була отримана в результаті аналізу ризиків, тобто:

- найменування загрози;
- об’єкт загрози;
- вразливості;
- вплив на властивості інформації;

- можливі наслідки;
- пріоритет ризику;
- ступінь впливу;
- контрміри.

2.2.6 Реалізація загрози

Після реалізації загрози переоцінюються такі показники:

- вартість активів;
- пріоритет ризику;
- ступінь впливу.

Процес управління ризиками можна наглядно відобразити на рисунку 2.4.

Рис 2.3 Процес управління ризиками

Оскільки переоцінка активів проводиться один раз на рік, то доцільно проводити переоцінку ризиків з такою ж частотою.

2.3 Впровадження СУРІБ

В першу чергу необхідно встановити критерії прийняття ризику та класифікувати ризики в залежності від величини можливих втрат для конкретного підприємства. Для адекватного вибору критеріїв оцінки ризиків необхідно спочатку визначити вартість активів. Це пояснюється тим, що встановивши критерії ризику без урахування їх вартості, всі ризики можуть потрапити в одну категорію, що буде не правильним. Тобто спочатку необхідно визначити вартість активів.

2.3.1 Визначення вартості активів

Вартість активів визначає власник інформації. Вартості активів приведені в таблиці 2.6.

Таблиця 2.6 – Вартість активів

№	Актив	Вартість(грн)
1	2	3
1	Організаційно-розпоряджувальна інформація	1000
2	Журнал обліку внутрішніх документів	4000
3	Інформація про послуги підприємства	0
4	Інформація про співробітників	8000
5	Уставна документація	4000
6	Журнал обліку та реєстрації вхідних і вихідних документів	4000
7	Трудові договори	10000
8	Фінансові відомості підприємства	120000
9	Договори, контракти	30000

Продовження таблиці 2.6

1	2	3
10	Відомості про охоронну сигналізацію	3000
11	Звіти про проведені реєстраційні дії	5000
12	Повна характеристика комп'ютерної та автомобільної техніки	3000
13	Звіти про проведення оглядів	4000
14	Звіти про кількість наданих послуг	4000

2.3.2 Встановлення критеріїв прийняття ризику

З таблиці 2.3 вартість всіх активів 200000 гривень. В результат аналізу ризиків будуть розраховані кількісні показники ризику. На основі цих показників необхідно встановити пріоритети ризиків та визначити адекватний рівень інвестицій для зниження ризику.

2.3.3 Оцінка рівня ризику

Для оцінки рівня ризику необхідно визначити: найменування загрози, об'єкт загрози, використані вразливості, вплив на властивості інформації, можливі наслідки. Типова модель загроз приведена в таблиці 2.7.

Таблиця 2.7 – Модель загроз

Найменування загрози	Об'єкт загрози	Вразливості	Вплив на інформацію (К, Ц, Д)	Можливі наслідки
1	2	3	4	5
Антропогенні загрози				
1 Крадіжка				
ключів електронного підпису	персонал, відвідувачі, обслуговуючий персонал	не витягування носія з ключем ЕЦП після закінчення роботи з СЕД, збереження ключів ЕЦП у загальнодоступному місці	К Ц Д	спотворення, розкриття інформації, матеріальні втрати

Продовження таблиці 2.7

1	2	3	4	5
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до носіїв інформації	К Ц Д	розкриття інформації, матеріальні втрати
інформації	персонал, відвідувачі, обслуговуючий персонал	збереження ключової інформації на жорстких дисках та в реєстрі	К Ц Д	розкриття інформації, матеріальні втрати
засобів доступу	персонал, відвідувачі, обслуговуючий персонал	збереження засобів доступу у загальнодоступному місці	К Ц Д	розкриття інформації, матеріальні втрати
технічних засобів	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К Ц Д	розкриття інформації, матеріальні втрати
2 Підміна				
документу при передачі	персонал, відвідувачі, обслуговуючий персонал	не захищеність комп'ютерної мережі	К Ц Д	розкриття інформації, матеріальні втрати
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К Ц Д	розкриття інформації, матеріальні втрати
ключів електронного підпису	персонал, відвідувачі, обслуговуючий персонал	не витягування носія з ключем ЕЦП після закінчення роботи з СЕД, збереження ключів ЕЦП у загальнодоступному місці	К Ц Д	розкриття інформації, матеріальні втрати
ОС та ПЗ	персонал, відвідувачі, обслуговуючий персонал	не належний контроль доступу до приміщень	К Ц Д	розкриття інформації, матеріальні втрати
3 Знищення				
носіїв інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
ПЗ, ОС, СУБД	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства

Продовження таблиці 2.7

1	2	3	4	5
інформації	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
технічних засобів	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
каналів зв'язку	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц Д	втрата інформації, припинення роботи підприємства
інформації при передачі каналами зв'язку	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	Ц	втрата інформації, припинення роботи підприємства
4 Несанкціонований доступ				
при технічному обслуговуванні (ремонті, знищенні) вузлів ПЕОМ	обслуговуючий персонал	відсутність контролю за технічним персоналом	К Ц Д	знищення, спотворення, розкриття інформації, матеріальні втрати
при передачі каналами зв'язку	персонал, відвідувачі, обслуговуючий персонал	недостатня захищеність комп'ютерної мережі	К Ц Д	знищення, спотворення, розкриття інформації, матеріальні втрати
5 несанкціоноване вимкнення засобів захисту	персонал, відвідувачі, обслуговуючий персонал	не належний контроль за діями працівників підприємства, відвідувачів та обслуговуючого персоналу	К Ц Д	втрата, розкриття інформації, матеріальні втрати

Продовження таблиці 2.7

1	2	3	4	5
6 Дія шкідливих програм(вірусів)	персонал, відвідувачі, обслуговуючий персонал	використання комп'ютерів, на яких встановлена СЕД для відвідування сторонніх Інтернет сайтів, встановлення несертифікованого ПЗ, не пов'язаного з виконанням службових обов'язків	К Ц Д	розкриття, втрата інформації, матеріальні втрати
7 Розголошення інф. співробітниками, допущеними до її обробки	персонал	погана інформованість співробітників з боку ІБ, зацікавленість в розкритті інформації	К Ц Д	розкриття інформації, матеріальні втрати
Техногенні загрози				
1 Знищення:				
носіїв інформації	пожежа, землетрус, старіння, збій системи електрозабезпечення	відсутність системи пожежогасіння, контролю за станом обладнання, системою електрозабезпечення	Ц	втрата інформації
засобів обробки інформації	пожежа, землетрус, старіння, збій системи електрозабезпечення	відсутність системи пожежогасіння, контролю за станом обладнання, системою електрозабезпечення	Ц Д	втрата інформації, припинення роботи підприємства
інформації(розмагнічування, радіація)	старіння, збій системи електрозабезпечення	відсутність контролю за станом обладнання, системою електрозабезпечення	Ц	втрата інформації
приміщень	пожежа, землетрус, старіння, збій системи електрозабезпечення	відсутність системи пожежогасіння, контролю за станом обладнання, системою електрозабезпечення	Ц	втрата інформації

2.3.4 Визначення пріоритетів ризику

На наступному етапі необхідно встановити річну частоту події, очікуваний одиничний збиток та визначити очікуваний річний збиток. На основі даної оцінки визначити пріоритет для кожного ризику. Результати оцінки приведені в таблиці 2.8.

Таблиця 2.8 – Пріоритети ризиків

Загроза	Річна частота події	Очікуваний одиничний збиток	Фактор впливу	Очікуваний річний збиток	Пріоритет ризику
1	2	3	4	5	6
Антропогенні загрози					
1. Крадіжка					
ключів електронного підпису	0,05	120000	0,3	1800	2
носіїв інформації	0,1	12000	0,3	360	3
інформації	0,15	12000	0,3	540	2
засобів доступу	0,05	12000	0,4	240	3
технічних засобів	0,2	12000	0,2	480	3
2. Підміна					
документу при передачі	0,1	10000	0,5	500	3
носіїв інформації	0,1	10000	0,6	600	2
ключів електронного підпису	0,05	120000	0,4	2400	2
ОС та ПЗ	0,05	12000	0,5	300	3
3. Знищення					
носіїв інформації	0,05	5000	0,4	100	3
ПЗ, ОС, СУБД	0,05	12000	0,5	300	3
інформації	0,1	12000	1	1200	2
технічних засобів	0,1	12000	0,4	480	3
каналів зв’язку	0,05	12000	0,2	120	3
інформації при передачі каналами зв’язку	0,05	12000	0,6	360	3
4. Несанкціонований доступ					
при технічному обслуговуванні (ремонті, знищенні) вузлів ПЕОМ	0,2	10000	0,5	1000	2
при передачі каналами зв’язку	0,1	8000	0,2	160	3
5. несанкціоноване вимкнення засобів захисту	0,15	30000	0,4	1800	2
6. Дія шкідливих програм(вірусів)	0,2	30000	0,6	3600	1
7. Розголошення інф. співробітниками, допущеними до її обробки	0,2	10000	0,6	1200	2
Техногенні загрози					
1. Знищення:					
носіїв інформації	0,1	50000	0,6	6000	1
засобів обробки інформації	0,2	5000	0,3	300	3
інформації(розмагнічування, радіація)	0,2	10000	0,6	1200	2
приміщень	0,1	120000	0,3	3600	1
2. Вихід з ладу вузлів ПЕОМ, каналів зв’язку	0,2	8000	0,3	480	3

2.3.5 Визначення мір зі зниження ризиків

На даному етапі необхідно визначити міри зі зниження ризиків, встановити їх вартість та адекватність. Тобто необхідно визначити рівень ризику після прийняття мір, порівняти його з початковим рівнем ризику та визначити ефективність. Результати приведені в таблиці 2.6

Таблиця 2.9 – Міри зі зниження ризику

Загроза	Рівень ризику	Міри зі зниження ризику	Пріоритет ризику
1	2	3	4
Антропогенні загрози			
1. Крадіжка			
ключів електронного підпису	1800	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	
носіїв інформації	360	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	
інформації	540	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	
засобів доступу	240	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	
технічних засобів	480	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	

Продовження таблиці 2.9

технічних засобів	480	контроль доступу до приміщення, інструктаж з ІБ, контроль доступу до серверної	
2. Підміна			
документу при передачі	500	ЕЦП	
носіїв інформації	600	облік носіїв інформації, контроль доступу до приміщень	
ключів електронного підпису	2400	інструктаж з ІБ	
ОС та ПЗ	300	контроль доступу до приміщення	
3. Знищення			
носіїв інформації	100	резервне копіювання, контроль доступу до серверної	

ПЗ, ОС, СУБД	300	резервне копіювання	
інформації	1200	резервне копіювання, розмежування прав, контроль доступу до серверної	
технічних засобів	480	резервне копіювання	
каналів зв'язку	120	резервне копіювання	
інформації при передачі каналами зв'язку	360	резервне копіювання	
4. Несанкціонований доступ			
при технічному обслуговуванні (ремонті, знищенні) вузлів ПЕОМ	1000	контроль за обслуговуючим персоналом,	
при передачі каналами зв'язку	160	шифрування	
5. несанкціоноване вимкнення засобів захисту	1800	контроль доступу до серверної	
6. Дія шкідливих програм(вірусів)	3600	антивірус, фаєрвол, інструктаж з ІБ	
7. Розголошення інф. співробітниками, допущеними до її обробки	1200	інструктаж з ІБ, обговорення в договорі наслідки в разі розголошення ІзОД	
Техногенні загрози			
1. Знищення:			
носіїв інформації	6000	резервне копіювання, контроль за станом обладнання, блок безперебійного живлення	
засобів обробки інформації	300	резервне копіювання, контроль за станом обладнання, блок безперебійного живлення	
інформації(розмагнічування, радіація)	1200	резервне копіювання, контроль за станом обладнання, блок безперебійного живлення	
приміщень	3600	резервне копіювання, контроль за станом обладнання	

2.3.6 Перелік запропонованих мір до впровадження

Далі необхідно встановити міри, які найбільш ефективно знижують ризик, та будуть запропоновані до впровадження з метою зниження ризиків, які мають високий рівень впливу. Також необхідно врахувати міри, які впливають не лише на один ризик а на декілька, тим самим знижуючи декілька ризиків.

Таблиця 2.10 – Першочергові міри зі зниження ризику

Міри	Характеристика	Вартість
Резервне копіювання		360
Блок безперервного живлення		450
Кодовий замок на серверну	Satel SZW-02, встановлюється своїми силами	342
Облік носіїв інформації	Створення журналу(4 год., переоблік раз на тиждень)	156
Контроль стану обладнання	Контроль носіїв, ПК, каналів звязку	676
Інструктаж з ІБ	Проводить системний адміністратор, раз на пів року	82
Фаєрвол	Outpost Firewall	197(98/рік)
Антивірус	Eset Nod Smart Security	510/рік

Висновок

Були проаналізовані проблеми у сфері інформаційної безпеки, можливі загрози інформаційній безпеці, що впливають на функціонування систем електронного документообігу.

Також була запропонована модель управління інформаційними ризиками в системах електронного документообігу та створена типова модель загроз.

В спеціальній частині були проаналізовані ризики, запропоновані міри зі зниження ризиків та визначені першочергові заходи.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Метою дипломної роботи є забезпечення захисту формації, циркулюючої в системах електронного документообігу шляхом впровадження системи управління ризиками.

Витоки/втрати інформації, яка є критично важливими для кожного підприємства, несуть за собою матеріальні збитки.

Метою економічного розділу є визначення економічної доцільності впровадження запропонованих мір зі зниження ризиків.

Задачами економічного розділу є встановлення:

– витрат на придбання і налагодження мір зі зниження ризиків в установі;

– річних експлуатаційних витрат, необхідних для підтримання та ефективного функціонування придбаних.

– оцінка економічної ефективності.

3.2 Розрахунок капітальних витрат

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

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

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

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

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

$К_{н}$ – витрати на встановлення та налагодження прийняття мір протидії витокам інформації, грн;

$К_{зпз}$ –вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації: резервне копіювання, блок безперервного живлення,

кодовий замок, журнал обліку носіїв інформації, контроль стану обладнання, інструктаж з ІБ, Firewall Analyzer Standard Edition, ESET Internet Security.

3.2.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням кодового замка, встановленням фаєрволу, антивірусу та обліком носіїв інформації займаєть системний адміністратор.

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

$$З = ТС* Ф , \quad (3.2)$$

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

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 140 грн/год.

Час на налагодження резервного копіювання займе 1 год.

$$З = ТС* Ф = 140*1=140, грн$$

Час на встановлення блоку безперервного живлення займе 0,5 год, затрати:

$$З = ТС* Ф = 140*0,5=70, грн$$

Час на встановлення кодового замку займе 1 год, затрати:

$$З = ТС* Ф = 140*1=140, грн$$

Час на встановлення фаєрволу займе 0,5 год, затрати:

$$З = ТС* Ф = 140*0,5=70, грн.$$

Час на встановлення антивірусу займе 0,5 год, затрати:

$$З = ТС* Ф = 140*0,5=70, грн$$

Час на створення журналу обліку носіїв займе 4 год, затрати:

$$З = ТС* Ф = 140*4=560, грн$$

3.2.2 Розрахунок капітальних витрат

В таблиці 4.1 наведена кількісно-вартісна характеристика заходів, що впроваджується в підприємстві великого бізнесу.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість
Резервне копіювання	SSD Samsung T7 2TB Shield Blue (MU-PE2T0R) 2022, up to 1050MB/s, www.rozetka.com.ua	11799
Блок безперервного живлення	Powercom BNT-800AP USB, www.rozetka.com.ua	5198
Кодовий замок на серверну	RZ M-1603BK-30, встановлюється своїми силами, www.rozetka.com.ua	755
Облік носіїв інформації	Створення журналу(4 год., переоблік раз на тиждень)	356
Фаєрвол	Firewall Analyzer Standard Edition, hhttps://www.fortsoft.com.ua/	15405
Антивірус	ESET Internet Security www.rozetka.com.ua	1049

Фіксовані витрати на проектування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 140 + 11799 = 11939(грн)$$

Блок безперервного живлення:

$$К = 70 + 5198 = 5268 (грн)$$

Кодовий замок на серверну:

$$К = 140 + 755 = 895 (грн)$$

Облік носіїв інформації:

$$К = 356 (грн)$$

Фаєрвол:

$$К = 70 + 15405 = 15475 (грн)$$

Антивірус:

$$К = 70 + 1049 = 1119 (грн)$$

Загальні затрати складуть 35052 грн.

3.3 Розрахунок поточних (експлуатаційних) витрат

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

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

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

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на замок на серверну;
- витрати на ліцензію фаєрволу;
- витрати на блок безперебійного живлення;
- витрати на облік носіїв інформації;

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

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

де С – вартість підстримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою фаєрволу, антивірусу та обліком носіїв інформації займаєть системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА}$=140 грн/год.

Час на резервного копіювання займе 0,1 год /день.

$$С = ТС* Ф = 140*0,1*250=3500 грн$$

Час на підтримку фаєрволу займе 0,2 год/тиждень, затрати:

$$С = ТС* Ф = 140*0,2*50=1400 грн$$

Час на підтримку антивірусу займе 0,2 год/тиждень, затрати:

$$С = ТС* Ф = 140*0,2*50=1400 грн$$

Час на створення журналу обліку носіїв займе 1 год/тиждень, затрати:

$$С = ТС* Ф = 140*1*50=7000 грн$$

Затрати на продовження ліцензії антивірусу складають 630 грн.

Затрати на продовження ліцензії фаєрволу складають 6162 грн.

Значення загальних річних поточних витрат складає:

$$С = 3500 + 1400 + 1400+ 7000 + 630 + 6162 = 20 092 (грн)$$

3.4 Оцінка можливого збитку від порушення інформаційної безпеки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

3.5 Визначення збитку від поломок обладнання

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

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п$ = 3 год;
- час відновлення після поломки, $t_в$ (в годинах), $t_в$ = 2 год;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви}$ = 1 год;
- заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), Z_0 = 15000 грн.;
- заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 20000 грн.;
- кількість обслуговуючого персоналу, N_0, N_0 = 2;
- число співробітників, N_c, N_c = 56;
- прибуток , O (грн. на рік), O = 8500000 грн.;
- вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 0 грн;
- число зламаного обладнання, I, I = 1;
- число поломок на рік, n, n = 7.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

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

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (56*20000/160)*3 = 21000 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

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

де $П_{ви}$ – вартість повторного введення інформації(формула 3.12),

$П_{пв}$ – вартість відновлення обладнання(формула 3.13).

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

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

Отримаємо:

$$П_{ви} = (56*20000/160)*1 = 7000 \text{ грн.}$$

$$П_{пв} = (2*15000/160)*2 = 375 \text{ грн.}$$

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

$$П_{зч} = 0 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 7000 + 375 + 0 = 7375 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

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

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

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

$$V = (8500000/2080)*(3+2+1) = 24519{,}23 \text{ грн.}$$

$$U = 21000 + 7375 + 24519{,}23 = 52894{,}23 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_{n}\sum_{I} U \text{, грн.} \quad (3.10)$$

ОУ = 7 * 1 * 52894,23 = 370 259,61 грн.

3.6 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу, визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

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

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

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

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компаній, що реалізують послуги аутсорсингу, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 370\,259{,}61 * 0{,}4 - 20\,092 = 128\,011{,}84 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за

формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

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

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

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

Підставивши відповідні значення, маємо:

$$ROSI = 128011,84 / 35052 = 3,65$$

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

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.20:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.13)$$

де $N_{деп}$ – річна депозитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Підставивши відповідні значення, маємо:

$$ROSI > (17 - 21,8)/100),$$

$$3,65 > -0,048$$

Отже, проект є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 1 / 3,65 = 0,27 \text{ року.}$$

Висновок

Розрахувавши збитки від реалізації можливих несправностей, які склали 370 259,61 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 20 092 грн., та витратами на розробку моделі 35 052 грн., можна зробити висновок, що витрати на забезпечення

інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом, термін окупності системи безпеки становить 0,27 року. Для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

У даній магістерської роботі були сформовані вимоги та визначений метод управління ризиками в системах електронного документообігу на об'єкті інформаційної діяльності.

У ході роботи було проведено аналіз систем електронного документообігу з точки зору інформаційгої безпеки.

Також були проаналізовані моделі аналізу ризиків та обрана оптимальна модель для даного підприємства.

Було розроблено типову модель загроз, рекомендації по впровадженню системи управління ризиків в системах електронного документообігу та приведений приклад впровадження системи.

Також була доведена економічна доцільність впровадження визначених організаційних заходів для забезпечення зниження рівнів ризику в системах електронного документообігу.

В роботі було детально розглянуто модель кількісну модель оцінки ризиків «очікуваний річний збиток».

Пропозиції можуть бути прийняті, як базові для підрозділів державної інспекції архітектури та містобудування України.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України про інформацію.
2. Закон України про Про захист інформації в інформаційно-комунікаційних системах.
3. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги.
4. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова.
5. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання.
6. ДСТУ ISO/IEC 27001:2010 Система управління інформаційною безпекою. Вимоги.
7. ISO/IEC 27035:2011 Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки.
8. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі.
9. НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
10. ДСТУ ISO/IEC 27002:2010 Звід правил для управління інформаційною безпекою.
11. НД ТЗІ 1.6-005-2013 Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
12. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека) / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. –

Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2011. – 17 с.

13. ДСТУ-Н Б А.3.2-1:2007 Система стандартів безпеки праці.
14. ДСТУ Б В.1.1-36:2016 Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою.
15. Microsoft (Електрон. ресурс) / Спосіб доступу: URL: https://www.microsoft.com/

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітка
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	28	
6	А4	Спеціальна частина	16	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік матеріалів на USB-flash drive	1	
12	А4	Додаток Г. Відгук керівника дипломної роботи	2	
13	А4	Додаток В. Відгуки керівників розділів	1	
14	А4	Додаток Д. Акт на категорювання інформації	2	

ДОДАТОК Б. Перелік матеріалів на USB-flash drive

1 Пояснювальна записка.(Кримчак Пояснювальна записка.docx)

2 Презентація.(Кримчак Презентація.pptx)

ДОДАТОК В. Відгуки керівників розділів

В.1 Відгук керівника економічного розділу

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

Відгук
керівника кваліфікаційної роботи магістра на тему:
“Розробка моделі управління ризиками інформаційної безпеки в системі електронного документообігу об’єкта критичної інфраструктури”
студента групи125м-21з-1Кримчака Павла Вадимовича

Мета дипломної роботи – забезпечити рівень безпеки інформації, циркулюючої в системах електронного документообігу шляхом впровадження системи управління ризиками.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності спеціальності 125 Кібербезпека – розробкою та впровадженням систем інформації.

Задачі дипломної роботи (аналіз методів управління ризиками, аналіз загроз інформаційній безпеці компанії в системах електронного документообігу, встановлення моделі управління ризиками компаній даного типу, розробка рекомендацій з впровадження моделі управління ризиками, розробка рекомендацій зі зниження ризиків) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Наукова новизна полягає у тому, що розроблені рекомендації можна застосовувати на практиці до ІС будь-якого відділу підприємства.

Практичне значення результатів проектування полягає у запропонуванні ефективного рішення щодо управління ризиками в системах електронного документообігу з урахуванням специфіки діяльності компанії.

Оформлення пояснювальної записки до дипломної роботи виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи добра.

За час дипломування Кримчак Павло Вадимович виявив себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “_____”, а Кримчак Павло Вадимович присвоєння йому кваліфікації магістра з кібербезпеки.

Керівник дипломної роботи,
д.т.н., професор _____ **В.І.Корнієнко**
(підпис)

ДОДАТОК Д

ФОРМА ТА ЗМІСТ АКТА КАТЕГОРІЮВАННЯ ОБ'ЄКТА

Гриф обмеження доступу для службового користування

Прим. № ___

ЗАТВЕРДЖУЮ

Керівник установи-власника (розпорядника, користувача) об'єкта

Голова С.Кривоніс

(посада, підпис, ініціали, прізвище)

____. ____. 20___

М.П.

АКТ

категоріювання державна інспекція архітектури та містобудування України

(найменування об'єкта категоріювання)

1. Підстава для категоріювання на об'єкт циркулює інформація з обмеженим доступом

(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

(обробка інформації технічними засобами та/або озвучування інформації)

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

(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 четверта

Голова комісії П.Кримчак

(підпис) (ініціали, прізвище)

Члени комісії: І.Прусенко

(підпис) (ініціали, прізвище)

____._____. 2022р