

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

**на тему: «DLP-система захисту інформації організації від витоку
інформації»**

здобувача: Веремейчук Анни Володимирівни _____

Науковий керівник: к.т.н., доц. Мирутенко Л. В. _____

**Робота допущена до захисту перед екзаменаційною комісією з
атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А. _____

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

_____ А. В. Бегун

(підпис) (ініціали, прізвище)

_____ 2026 р.

ЗАТВЕРДЖУЮ:

Завідувач кафедри

_____ І.А. Джалладова

(підпис) (ініціали, прізвище)

_____ 2026 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти: Веремейчук Анни Володимирівни

_____ очної (денної) _____ форми навчання

на підготовку кваліфікаційної бакалаврської роботи

**на тему: « DLP-система захисту інформації організації від витоку
інформації »**

Тему затверджено наказом ректора Університету від «___» _____ 20__ р. №__

Кваліфікаційна бакалаврська робота виконується на матеріалах

ПЛАН КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ РОБОТИ

Розділ 1 | Теоретичні основи захисту інформації від внутрішніх загроз

(назва розділу)

Розділ 2 | Аналіз інформаційної системи підприємства та загроз

(назва розділу)

Розділ 3 | Розробка системи захисту інформації із застосуванням DLP-технологій

(назва розділу)

Об'єкт дослідження: | процес забезпечення захисту інформації організації від витоку інформації.

Предмет дослідження: | методи, засоби та технології запобігання витоку інформації з використанням DLP-систем.

Мета кваліфікаційної

бакалаврської роботи: | розробити систему захисту інформації організації від витоку даних із застосуванням DLP-технологій на основі аналізу інформаційної інфраструктури підприємства, внутрішніх загроз, інформаційних активів та каналів можливого витоку інформації.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1| необхідно проаналізувати теоретичні основи інформаційної безпеки, визначити сутність внутрішніх загроз, розглянути класифікацію внутрішніх порушників, дослідити поняття витоку інформації та охарактеризувати DLP-технології як засіб запобігання втраті даних.

У розділі 2| слід надати загальну характеристику підприємства МАК-SERVIS, проаналізувати його інформаційну інфраструктуру, визначити основні інформаційні активи, дослідити внутрішні загрози витоку інформації та оцінити систему контролю доступу до інформаційних ресурсів.

У розділі 3| потрібно побудувати модель внутрішнього порушника, визначити основні канали витоку інформації, розробити систему захисту на основі DLP-технологій, запропонувати практичні заходи захисту та оцінити ефективність запропонованих рішень.

Завдання підготував
науковий керівник

(підпис)

Мирутенко Л. В.
(прізвище, ініціали)

Завдання одержав
здобувач

(підпис)

Веремейчук А. В.
(прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна бакалаврська робота на тему: «DLP-система захисту інформації організації від витоку інформації».

Пояснювальна записка: 62 с., 20 рис., 7 табл., 45 джерел.

Об'єктом дослідження є процес забезпечення захисту інформації організації від витоку інформації.

Предметом дослідження є методи, засоби та технології запобігання витоку інформації із застосуванням DLP-систем.

Метою кваліфікаційної бакалаврської роботи є розробка системи захисту інформації організації від витоку даних із використанням DLP-технологій на основі аналізу інформаційної інфраструктури підприємства, внутрішніх загроз, інформаційних активів та можливих каналів витоку інформації.

У ході роботи було розглянуто поняття інформаційної безпеки, внутрішніх загроз та внутрішнього порушника. Проведено аналіз витоку інформації як однієї з основних загроз для організації, а також досліджено призначення, принцип роботи та можливості застосування DLP-технологій для захисту конфіденційних даних.

У практичній частині роботи проаналізовано інформаційну систему підприємства МАК-СЕРВІС. Було досліджено робочі станції, мережеві налаштування, інформаційні активи підприємства та систему контролю доступу. Визначено основні інформаційні активи, зокрема базу клієнтів, службові документи та робочі файли співробітників.

Під час дослідження виявлено основні внутрішні загрози витоку інформації: копіювання файлів на зовнішні носії, передача даних через мережу, доступ до інформації, яка не входить до службових обов'язків користувача, а також використання надлишкових прав доступу.

У роботі побудовано модель внутрішнього порушника, визначено можливі канали витоку інформації та запропоновано систему захисту на основі DLP-

технологій. Запропоновані заходи передбачають контроль використання зовнішніх носіїв, моніторинг дій користувачів, обмеження доступу до конфіденційної інформації та контроль передачі даних.

Наукова новизна роботи полягає в удосконаленні підходу до захисту інформації організації від витоку даних шляхом використання DLP-технологій з урахуванням моделі внутрішнього порушника та реальних каналів можливого витоку інформації.

Практична значущість роботи полягає у можливості використання запропонованої системи захисту для зниження ризику витоку конфіденційної інформації на підприємстві, посилення контролю доступу та підвищення рівня інформаційної безпеки організації.

Ключові слова: dlp-система, інформаційна безпека, витік інформації, внутрішній порушник, інформаційні активи, контроль доступу, конфіденційна інформація, моніторинг дій користувачів, зовнішні носії, захист даних.

ВІДГУК

на кваліфікаційну бакалаврську роботу

студента Веремейчук Анни Володимирівни гр. ІК-401

(прізвище, ім'я)

на тему: DLP-система захисту інформації організації від витоку інформації

Актуальність теми. Тема кваліфікаційної бакалаврської роботи є актуальною, оскільки в сучасних умовах діяльності підприємств значною мірою залежить від використання інформаційних систем, електронного документообігу, локальних мереж та цифрових засобів передавання даних. Особливої уваги потребує проблема витоку конфіденційної інформації, що може виникати не лише внаслідок зовнішніх атак, а й через дії внутрішніх користувачів. У роботі обґрунтовано необхідність застосування DLP-технологій як ефективного засобу контролю інформаційних потоків, моніторингу дій користувачів та запобігання несанкціонованому поширенню службових даних.

Повнота розкриття теми. Тема роботи розкрита достатньо повно. У першому розділі досліджено теоретичні основи інформаційної безпеки, внутрішні загрози, класифікацію внутрішніх порушників, канали витоку інформації та призначення DLP-систем. У другому розділі виконано аналіз інформаційної системи підприємства ТОВ «МАК-СЕРВІС», визначено інформаційні активи, місця їх зберігання, потенційні канали витоку та недоліки існуючої системи контролю доступу. У третьому розділі розроблено практичні рішення щодо захисту інформації, побудовано модель внутрішнього порушника, обґрунтовано вибір DLP-системи SearchInform DLP, запропоновано архітектуру системи захисту та політики контролю інформаційних потоків.

Теоретичний рівень. Теоретичний рівень роботи є достатнім для кваліфікаційної бакалаврської роботи. Здобувачка опрацювала наукову, навчальну, нормативну та електронну літературу з питань інформаційної безпеки, внутрішніх загроз, DLP-технологій та захисту інформаційних ресурсів підприємства. У роботі правильно розкрито основні поняття, пов'язані з

конфіденційністю, цілісністю, доступністю інформації, внутрішніми порушниками, каналами витоку інформації та засобами їх контролю. Теоретичний матеріал логічно пов'язаний із практичною частиною дослідження.

Практична значущість. Практична значущість роботи полягає у розробці системи захисту інформації для ТОВ «МАК-СЕРВІС» із застосуванням DLP-технологій. У роботі запропоновано конкретні заходи щодо контролю USB-пристроїв, електронної пошти, конфіденційних документів, журналювання подій та сповіщення адміністратора про інциденти інформаційної безпеки. Розроблені схеми, таблиці та політики безпеки можуть бути використані як основа для подальшого впровадження системи контролю витоку інформації на підприємстві.

Самостійність виконання роботи. Робота свідчить про достатній рівень самостійності здобувачки під час виконання дослідження. Авторкою самостійно проведено аналіз інформаційної інфраструктури підприємства, визначено основні інформаційні активи, внутрішні загрози та канали можливого витоку інформації. Також самостійно побудовано модель внутрішнього порушника, виконано порівняння DLP-систем, обґрунтовано вибір SearchInform DLP та розроблено практичні заходи захисту інформації.

Якість оформлення, загальна та спеціальна грамотність. Кваліфікаційна бакалаврська робота має логічну структуру, складається зі вступу, трьох розділів, висновків та списку використаних джерел. Матеріал викладено послідовно, з використанням фахової термінології у сфері кібербезпеки та захисту інформації. У роботі використано таблиці, схеми та рисунки, які доповнюють текст і відображають результати аналізу та розробки системи захисту. Загалом робота оформлена відповідно до вимог, однак окремі формулювання та технічні елементи оформлення потребують додаткового уважного редагування перед остаточним поданням.

Переваги та недоліки роботи. До переваг роботи слід віднести актуальність обраної теми, логічну структуру дослідження, поєднання теоретичного аналізу з практичними результатами, наявність моделі внутрішнього порушника,

порівняльного аналізу DLP-систем та розроблених політик захисту інформації. Практична частина роботи має прикладне значення, оскільки орієнтована на конкретне підприємство та враховує виявлені під час аналізу загрози. До недоліків можна віднести те, що окремі запропоновані заходи мають проєктний характер і потребують подальшої практичної апробації в реальному середовищі підприємства. Також бажано було б розширити кількісну оцінку ефективності впровадження DLP-системи.

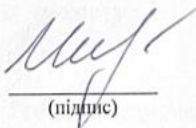
Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК. Кваліфікаційна бакалаврська робота Веремейчук Анни Володимирівни на тему «DLP-система захисту інформації організації від витoku інформації» є завершеним самостійним дослідженням, у якому вирішено поставлені завдання та досягнуто мету роботи. Робота має теоретичну та практичну значущість, відповідає вимогам до кваліфікаційних бакалаврських робіт за спеціальністю 125 «Кібербезпека» та може бути рекомендована до захисту перед екзаменаційною комісією. Робота заслуговує на позитивну оцінку.

Науковий керівник

к.т.н., доцент, доцент кафедри
системного аналізу та
кібербезпеки факультету
інформаційних технологій в
економіці

КНЕУ ім. Вадима Гетьмана

(посада)



(підпис)

Лариса МИРУТЕНКО

(ініціали, прізвище)

_____ червня 2026 року

РЕЦЕНЗІЯ
на кваліфікаційну бакалаврську роботу

студентки Веремейчук Анни Володимирівни гр. ІК - 401
(прізвище, ініціали)

на тему: DLP-система захисту інформації організації від витоку інформації

Актуальність теми. Тема кваліфікаційної бакалаврської роботи «DLP-система захисту інформації організації від витоку інформації» є актуальною та своєчасною. У сучасних умовах цифровізації діяльності підприємств питання забезпечення захисту інформаційних ресурсів набуває особливого значення. Однією з найбільш небезпечних загроз інформаційній безпеці є витік конфіденційної інформації внаслідок дій внутрішніх користувачів. Використання DLP-технологій дозволяє здійснювати контроль передачі даних, виявляти порушення політик безпеки та мінімізувати ризики втрати службової інформації. Тому обрана тема має практичне значення та відповідає сучасним потребам забезпечення кібербезпеки організацій.

Наукова новизна. Наукова новизна роботи полягає в комплексному підході до дослідження внутрішніх загроз інформаційній безпеці підприємства та розробці системи захисту інформації із застосуванням DLP-технологій. Автором проведено аналіз інформаційних активів підприємства, каналів можливого витоку інформації та побудовано модель внутрішнього порушника. Запропоновані рішення враховують особливості функціонування корпоративної інформаційної системи та сучасні підходи до захисту інформації від несанкціонованого розповсюдження.

Якість проведеного аналізу. Робота відзначається достатньо високим рівнем аналітичного опрацювання матеріалу. У дослідженні проведено аналіз інформаційної інфраструктури підприємства, локальної мережі, серверного обладнання, програмного забезпечення та механізмів контролю доступу. Визначено основні інформаційні активи, проаналізовано існуючі загрози та канали витоку інформації. Наведені таблиці, схеми та рисунки є інформативними,

логічно доповнюють текст роботи та сприяють кращому сприйняттю результатів дослідження. Висновки до розділів є обґрунтованими та відповідають отриманим результатам.

Уміння користуватися літературними джерелами. Автор продемонстрував належний рівень опрацювання наукової, навчальної та нормативно-правової літератури з питань інформаційної безпеки та захисту інформації. У роботі використано сучасні джерела, присвячені внутрішнім загрозам, DLP-технологіям, методам контролю доступу та запобігання витоку інформації. Посилання на джерела наведено коректно та використано для підтвердження основних положень дослідження.

Практична цінність висновків і рекомендацій. Практична цінність роботи полягає у розробленні комплексу заходів щодо підвищення рівня інформаційної безпеки підприємства шляхом впровадження DLP-системи SearchInform DLP. Запропоновані рішення дозволяють забезпечити контроль використання USB-носіїв, електронної пошти, мережевого трафіку, здійснювати моніторинг дій користувачів та журналювання подій інформаційної безпеки. Отримані результати можуть бути використані під час удосконалення систем захисту інформації на підприємствах малого та середнього бізнесу.

Переваги та недоліки. До основних переваг роботи слід віднести актуальність тематики, логічну структуру дослідження, комплексний аналіз інформаційної системи підприємства, наявність практичної складової та обґрунтований вибір DLP-рішення для впровадження. Позитивним є використання схем, моделей, порівняльних таблиць та оцінювання ефективності запропонованих заходів захисту. Серед окремих недоліків можна зазначити, що робота могла б бути доповнена більш детальним економічним обґрунтуванням впровадження DLP-системи та розширеним аналізом зарубіжного досвіду використання засобів запобігання витоку інформації. Однак зазначені зауваження не впливають на загальну позитивну оцінку роботи.

Загальний висновок і оцінка роботи. Кваліфікаційна бакалаврська робота на тему «DLP-система захисту інформації організації від витоку інформації» є завершеним самостійним дослідженням, виконаним на належному науково-методичному рівні. Робота відповідає вимогам, що висуваються до кваліфікаційних робіт за спеціальністю 125 «Кібербезпека», містить елементи наукової новизни та має практичне значення. Автор продемонстрував достатній рівень теоретичної підготовки та здатність вирішувати актуальні завдання у сфері захисту інформації. Кваліфікаційна бакалаврська робота заслуговує на оцінку «відмінно», а її автор — на присвоєння кваліфікації бакалавра за спеціальністю 125 «Кібербезпека».

Рецензент

*К.І.І. Даниш, завідувач кафедри Систем
Технологій М.Тараса Шевченка*

(посада)

[Підпис]

(підпис)

О.В. Ісакюк

(ініціали, прізвище)

“ ” 2026р.

Печатка



ЗМІСТ

ВСТУП	3
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ	6
1.1. Поняття інформаційної безпеки та внутрішніх загроз.....	6
1.2. Класифікація внутрішніх порушників	8
1.3. Витік інформації як основна загроза.....	10
1.4. DLP-технології як засіб захисту інформації	12
1.5. Висновки до розділу 1	14
РОЗДІЛ 2 АНАЛІЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА ТА ЗАГРОЗ.....	16
2.1. Загальна характеристика підприємства МАК-СЕРВІС	16
2.2. Аналіз інформаційної інфраструктури	17
2.3. Визначення інформаційних активів підприємства	27
2.4. Аналіз внутрішніх загроз витоку інформації.....	31
2.5. Аналіз системи контролю доступу.....	34
2.6. Висновки до розділу 2	35
РОЗДІЛ 3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ DLP-ТЕХНОЛОГІЇ.....	37
3.1. Побудова моделі внутрішнього порушника.....	37
3.2. Впровадження журналювання дій користувачів	39
3.3. Обґрунтування вибору DLP - системи.....	40
3.4. Розробка системи захисту на основі SearchInform DLP.....	44
3.5. Реалізація заходів захисту	48
3.6. Оцінка ефективності запропонованих заходів.....	52
3.7. Висновки до розділу 3	55
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	59

ВСТУП

Актуальність теми. У сучасних умовах діяльність більшості організацій безпосередньо залежить від використання інформаційних систем, комп'ютерних мереж, електронного документообігу та цифрових баз даних. Разом із розвитком інформаційних технологій збільшується кількість загроз, пов'язаних із витоком конфіденційної інформації. Особливу небезпеку становлять внутрішні загрози, оскільки працівники організації мають безпосередній доступ до інформаційних ресурсів, службових документів та баз даних підприємства.

Проведений аналіз сучасних засобів захисту інформації показав, що значна кількість досліджень присвячена мережевій безпеці, криптографічному захисту та захисту від зовнішніх атак. Однак питання запобігання витоку інформації внаслідок дій внутрішніх користувачів залишається актуальним. Основними проблемами є наявність надлишкових прав доступу, недостатній контроль передачі даних, використання зовнішніх носіїв інформації та відсутність постійного моніторингу дій користувачів.

Одним із найбільш ефективних засобів протидії витоку інформації є використання DLP-технологій (Data Loss Prevention), які дозволяють контролювати передачу конфіденційної інформації, виявляти спроби несанкціонованого копіювання даних та здійснювати моніторинг дій користувачів.

Таким чином, актуальним завданням є розробка DLP-системи захисту інформації організації від витоку інформації з урахуванням внутрішніх загроз, особливостей інформаційної інфраструктури підприємства та можливих каналів витоку даних.

Мета і завдання дослідження. Метою кваліфікаційної бакалаврської роботи є розробка DLP-системи захисту інформації організації від витоку даних на основі

аналізу інформаційної інфраструктури підприємства, внутрішніх загроз, інформаційних активів та можливих каналів витоку інформації.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз теоретичних основ інформаційної безпеки та внутрішніх загроз;
- дослідити класифікацію внутрішніх порушників та їх можливості;
- визначити основні канали витоку інформації в організації;
- проаналізувати інформаційну інфраструктуру підприємства МАК-СЕРВІС;
- дослідити інформаційні активи та систему контролю доступу підприємства;
- побудувати модель внутрішнього порушника;
- розробити систему захисту інформації із застосуванням DLP-технологій;
- оцінити ефективність запропонованих заходів захисту.

Об'єктом дослідження є процес забезпечення захисту інформації організації від витоку інформації.

Предметом дослідження є методи, засоби та технології запобігання витоку інформації із застосуванням DLP-систем.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи системного аналізу, порівняння, спостереження, аналізу інформаційних ризиків, моделювання внутрішнього порушника та аналізу каналів витоку інформації.

Теоретична і методична значущість отриманих результатів полягає в удосконаленні підходу до захисту інформації організації від витоку даних шляхом застосування DLP-технологій, побудови моделі внутрішнього порушника та визначення основних каналів витоку інформації. Отримані результати дозволяють систематизувати внутрішні загрози, пов'язані з передачею конфіденційних даних, використанням зовнішніх носіїв та надлишковими правами доступу користувачів.

Наукова новизна і практична значущість. Наукова новизна отриманих результатів полягає в удосконаленні підходу до захисту інформації організації від витоку даних шляхом застосування DLP-технологій з урахуванням внутрішніх загроз, моделі внутрішнього порушника та можливих каналів передачі конфіденційної інформації.

Практична значущість роботи полягає у можливості використання запропонованої системи захисту для контролю передачі даних, обмеження несанкціонованого доступу до інформаційних ресурсів, моніторингу дій користувачів та зниження ризику витоку конфіденційної інформації на підприємстві МАК-СЕРВІС.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ

1.1. Поняття інформаційної безпеки та внутрішніх загроз

У сучасних умовах розвитку інформаційних технологій інформація є одним із найважливіших ресурсів будь-якої організації. Функціонування підприємств значною мірою залежить від роботи інформаційних систем, локальних мереж, електронного документообігу, хмарних сервісів та цифрових засобів передачі даних. Водночас активне використання інформаційних технологій супроводжується зростанням кількості загроз інформаційній безпеці [4, ст. 28].

Інформаційна безпека є складовою загальної системи безпеки організації та спрямована на забезпечення захисту інформаційних ресурсів від внутрішніх і зовнішніх загроз. Основною метою інформаційної безпеки є забезпечення стабільного функціонування інформаційної системи та захист інформації від несанкціонованого доступу, зміни, знищення або витоку [12, ст. 18].

Основу інформаційної безпеки становлять три ключові принципи:

- конфіденційність;
- цілісність;
- доступність.

Конфіденційність передбачає обмеження доступу до інформації лише для авторизованих користувачів. Порухення конфіденційності призводить до витоку інформації або її розголошення стороннім особам [16, ст. 37].

Цілісність означає збереження правильності та незмінності інформації. Порухення цілісності може проявлятися у зміні, пошкодженні або підробці даних [11, ст. 42].

Доступність забезпечує можливість отримання доступу до інформаційних ресурсів у необхідний момент часу для авторизованих користувачів [13, ст. 57].

Сучасні інформаційні системи постійно піддаються різним загрозам. Загроза інформаційній безпеці — це потенційна можливість порушення конфіденційності, цілісності або доступності інформації [15, ст. 74].

Усі загрози інформаційній безпеці поділяються на зовнішні та внутрішні. До зовнішніх загроз належать:

- хакерські атаки;
- шкідливе програмне забезпечення;
- мережеві атаки;
- фішинг;
- несанкціонований доступ до системи [18, ст. 96].

До внутрішніх загроз належать дії працівників організації, які мають доступ до інформаційних ресурсів підприємства. Саме внутрішні загрози є одними з найбільш небезпечних, оскільки внутрішній користувач уже має певний рівень доступу до системи та володіє інформацією про особливості її роботи [13, ст. 102].

Внутрішні загрози можуть бути навмисними або ненавмисними. Навмисні загрози виникають у випадках свідомого порушення політики безпеки працівником. Ненавмисні загрози пов'язані з помилками користувачів, недостатнім рівнем підготовки або порушенням правил роботи з інформацією [12, ст. 91].

Основними внутрішніми загрозами є:

- копіювання конфіденційних файлів;
- передача службової інформації стороннім особам;
- використання зовнішніх носіїв інформації;
- видалення або зміна даних;
- використання надлишкових прав доступу [11, ст. 118].

У більшості сучасних організацій внутрішні загрози становлять значний ризик через недостатній контроль дій користувачів, відсутність моніторингу передачі даних та неправильний розподіл прав доступу. Особливо небезпечними є

ситуації, коли працівники мають доступ до інформації, яка не пов'язана з виконанням їхніх службових обов'язків [16, ст. 124].

Одним із найбільш ефективних засобів захисту від внутрішніх загроз є використання DLP-систем (Data Loss Prevention), які дозволяють контролювати передачу інформації, виявляти спроби копіювання файлів, обмежувати використання зовнішніх носіїв та здійснювати моніторинг дій користувачів у корпоративній мережі [38].

Забезпечення інформаційної безпеки організації потребує комплексного підходу, який включає технічні, програмні та організаційні засоби захисту інформації. Особливу увагу необхідно приділяти внутрішнім загрозам, оскільки саме вони часто стають причиною витоку конфіденційної інформації та порушення безпеки інформаційних ресурсів підприємства.

1.2. Класифікація внутрішніх порушників

Однією з основних проблем забезпечення інформаційної безпеки організації є наявність внутрішніх порушників, які мають доступ до інформаційних ресурсів підприємства та можуть здійснювати дії, що призводять до витоку, пошкодження або втрати інформації. На відміну від зовнішніх зловмисників, внутрішні користувачі вже мають певний рівень доступу до інформаційної системи, володіють інформацією про особливості її функціонування та можуть обходити окремі механізми захисту [12, ст. 83].

Внутрішнім порушником є особа, яка має законний доступ до інформаційної системи підприємства та внаслідок навмисних або ненавмисних дій порушує встановлені правила інформаційної безпеки [13, ст. 102].

До внутрішніх порушників можуть належати:

- штатні працівники підприємства;
- системні адміністратори;
- керівники структурних підрозділів;
- тимчасові працівники;

- підрядники та сторонні спеціалісти, які мають доступ до корпоративної мережі або інформаційних ресурсів [11, ст. 117].

Класифікація внутрішніх порушників може здійснюватися за різними ознаками: рівнем доступу до інформації, мотивами дій, характером порушення та рівнем обізнаності щодо роботи інформаційної системи підприємства.

За рівнем доступу внутрішніх порушників поділяють на:

- користувачів із мінімальними правами доступу;
- користувачів із розширеними правами;
- адміністраторів системи;
- осіб із повним доступом до інформаційних ресурсів [16, ст. 158].

Користувачі з мінімальними правами мають доступ лише до тієї інформації, яка необхідна для виконання службових обов'язків. Такі користувачі не можуть змінювати налаштування системи або отримувати доступ до критично важливих ресурсів підприємства.

Користувачі з розширеними правами мають доступ до більшої кількості інформаційних ресурсів, корпоративної документації, баз даних та внутрішніх сервісів підприємства.

Найбільш небезпечними внутрішніми порушниками є системні адміністратори та користувачі з повним рівнем доступу. Такі особи можуть змінювати конфігурацію системи, створювати нові облікові записи, змінювати права доступу користувачів та отримувати доступ до конфіденційної інформації [18, ст. 143].

За мотивами дій внутрішніх порушників можна поділити на:

- навмисних;
- ненавмисних.

Навмисні порушники свідомо здійснюють дії, спрямовані на викрадення, передачу або пошкодження інформації. Основними мотивами можуть бути фінансова вигода, помста, конфлікти з керівництвом або передача інформації конкурентам [15, ст. 204].

Ненавмисні порушники не мають на меті завдати шкоди інформаційній системі підприємства. Порушення інформаційної безпеки в таких випадках виникає через неуважність, недостатній рівень підготовки, помилки під час роботи з інформацією або недотримання правил інформаційної безпеки [12, ст. 96].

До найбільш поширених дій внутрішніх порушників належать:

- копіювання файлів на зовнішні носії;
- передача конфіденційної інформації через електронну пошту;
- використання незахищених каналів зв'язку;
- встановлення стороннього програмного забезпечення;
- використання чужих облікових записів;
- видалення або зміна службових даних [11, ст. 136].

У більшості випадків причиною реалізації внутрішніх загроз є недостатній контроль дій користувачів, відсутність моніторингу передачі даних та наявність надлишкових прав доступу. Саме тому сучасні організації використовують DLP-системи, які дозволяють контролювати дії користувачів, виявляти спроби витоку інформації та блокувати передачу конфіденційних даних [38].

Внутрішні порушники становлять одну з найбільш небезпечних категорій загроз інформаційній безпеці організації. Ефективний захист інформаційних ресурсів потребує контролю дій користувачів, правильного розмежування прав доступу та використання сучасних засобів моніторингу й запобігання витоку інформації.

1.3. Витік інформації як основна загроза

У сучасних умовах розвитку інформаційних технологій витік інформації є однією з найбільш небезпечних загроз інформаційній безпеці організації. Значна кількість службових документів, баз даних, персональних даних та іншої конфіденційної інформації зберігається й передається в електронному вигляді, що суттєво підвищує ризик її несанкціонованого поширення [4, ст. 74].

Витік інформації — це неконтрольоване або несанкціоноване поширення інформації за межі організації чи кола осіб, які мають право доступу до неї. Наслідком витоку інформації можуть бути фінансові збитки, порушення роботи підприємства, втрата ділової репутації та розголошення конфіденційних даних [12, ст. 112].

Основними причинами витоку інформації є:

- недостатній контроль дій користувачів;
- наявність надлишкових прав доступу;
- відсутність моніторингу передачі даних;
- використання незахищених каналів зв'язку;
- недотримання правил інформаційної безпеки працівниками [16, ст. 203].

У більшості випадків витік інформації пов'язаний саме з внутрішніми користувачами, які мають доступ до інформаційних ресурсів підприємства. Внутрішні порушники можуть копіювати файли, передавати дані через електронну пошту, використовувати зовнішні носії або здійснювати несанкціоноване розповсюдження конфіденційної інформації [13, ст. 184].

Основними каналами витоку інформації є:

- зовнішні носії інформації;
- електронна пошта;
- хмарні сервіси;
- локальна мережа;
- мобільні пристрої;
- месенджери та інтернет-сервіси [18, ст. 166].

Одним із найбільш поширених способів витоку інформації є копіювання файлів на зовнішні носії інформації, зокрема USB-накопичувачі. У разі відсутності контролю використання зовнішніх носіїв працівник може швидко скопіювати значний обсяг конфіденційної інформації без виявлення такого порушення [11, ст. 141].

Також значну небезпеку становить передача службової інформації через електронну пошту або хмарні сервіси. У деяких випадках працівники використовують особисті поштові скриньки або сторонні файлові сервіси для передачі документів, що створює додаткові ризики витоку даних [37, ст. 73].

Витік інформації може бути як навмисним, так і ненавмисним. Навмисний витік інформації здійснюється з метою отримання фінансової вигоди, передачі інформації конкурентам або нанесення шкоди підприємству. Ненавмисний витік виникає через помилки користувачів, недостатній рівень підготовки персоналу або порушення правил роботи з інформацією [15, ст. 241].

Однією з головних проблем сучасних організацій є недостатній рівень контролю передачі конфіденційної інформації. У багатьох випадках підприємства використовують лише базові засоби захисту, які не дозволяють контролювати дії користувачів або виявляти спроби витоку даних [12, ст. 126].

Для запобігання витоку інформації використовуються DLP-системи (Data Loss Prevention), які дозволяють контролювати передачу файлів, аналізувати дії користувачів, обмежувати використання зовнішніх носіїв та блокувати передачу конфіденційної інформації через мережу [38].

Витік інформації є однією з основних загроз інформаційній безпеці організації. Для ефективного захисту інформаційних ресурсів необхідно здійснювати контроль дій користувачів, обмежувати канали передачі даних та використовувати сучасні засоби моніторингу й запобігання витоку інформації.

1.4. DLP-технології як засіб захисту інформації

У сучасних умовах розвитку інформаційних технологій та збільшення кількості внутрішніх загроз особливого значення набувають засоби контролю та запобігання витоку конфіденційної інформації. Одним із найбільш ефективних рішень у сфері захисту інформації є використання DLP-технологій (Data Loss Prevention), які забезпечують контроль передачі даних та запобігають несанкціонованому поширенню інформації [12, ст. 143].

DLP-система — це програмно-апаратний комплекс, призначений для виявлення, моніторингу та блокування передачі конфіденційної інформації за межі інформаційної системи організації [13, ст. 214].

Основною метою використання DLP-технологій є:

- контроль передачі конфіденційної інформації;
- виявлення спроб витоку даних;
- моніторинг дій користувачів;
- запобігання несанкціонованому копіюванню файлів;
- контроль використання зовнішніх носіїв інформації [16, ст. 241].

Сучасні DLP-системи дозволяють контролювати різні канали передачі інформації, серед яких:

- електронна пошта;
- USB-носії;
- локальна мережа;
- хмарні сервіси;
- месенджери;
- веб-сервіси та інтернет-ресурси [38].

Принцип роботи DLP-систем базується на аналізі інформації, яка передається через інформаційну систему підприємства. Під час передачі файлів або повідомлень система аналізує їх вміст, визначає наявність конфіденційної інформації та приймає рішення щодо дозволу або блокування передачі даних [39, ст. 96].

Для визначення конфіденційної інформації DLP-системи можуть використовувати:

- ключові слова;
- шаблони документів;
- цифрові відбитки файлів;
- аналіз структури документа;
- аналіз поведінки користувачів [37, ст. 112].

Однією з основних переваг DLP-технологій є можливість постійного моніторингу дій користувачів. Система фіксує передачу файлів, використання зовнішніх носіїв, надсилання повідомлень та інші дії, пов'язані з обробкою інформації [11, ст. 173].

Крім технічного контролю, DLP-системи дозволяють формувати журнали подій та звіти про потенційні порушення інформаційної безпеки. Це дозволяє адміністраторам системи оперативно виявляти спроби витоку інформації та аналізувати дії користувачів [13, ст. 228].

Сучасні DLP-рішення можуть працювати як у локальних мережах підприємства, так і в хмарному середовищі. До найбільш відомих DLP-систем належать:

- Symantec DLP;
- Forcepoint DLP;
- SearchInform DLP;
- McAfee Total Protection for DLP;
- Microsoft Purview DLP [27; 31; 40].

Незважаючи на значну ефективність DLP-технологій, їх впровадження потребує правильного налаштування політик безпеки, розмежування прав доступу та визначення конфіденційної інформації, яка підлягає контролю. Недостатньо налаштована система може створювати велику кількість помилкових спрацювань або не виявляти окремі загрози [37, ст. 148].

DLP-технології є одним із найбільш ефективних засобів захисту інформації від витоку даних та внутрішніх загроз. Використання таких систем дозволяє здійснювати контроль передачі інформації, моніторинг дій користувачів та запобігати несанкціонованому поширенню конфіденційної інформації в інформаційній системі організації.

1.5. Висновки до розділу 1

У першому розділі було досліджено теоретичні основи захисту інформації від внутрішніх загроз. Розглянуто поняття інформаційної безпеки, внутрішніх загроз та внутрішніх порушників, а також визначено їх вплив на безпеку інформаційних ресурсів підприємства.

У ході дослідження проаналізовано основні канали витоку конфіденційної інформації, серед яких електронна пошта, USB-носії, локальна мережа та хмарні сервіси. Встановлено, що відсутність контролю передачі даних створює значні ризики для інформаційної безпеки організації.

Також було досліджено принципи роботи DLP-систем та визначено їх основні функції щодо контролю передачі інформації, моніторингу дій користувачів і запобігання витоку конфіденційних даних.

Отже, проведений теоретичний аналіз підтвердив актуальність впровадження DLP-технологій для підвищення рівня захисту інформації підприємства від внутрішніх загроз та витоку інформації.

РОЗДІЛ 2

АНАЛІЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА ТА ЗАГРОЗ

2.1. Загальна характеристика підприємства МАК-СЕРВІС

Базою проходження переддипломної практики та об'єктом дослідження у кваліфікаційній бакалаврській роботі є підприємство ТОВ «МАК-СЕРВІС». Основна діяльність підприємства пов'язана з використанням інформаційних технологій, електронного документообігу, обробкою службової інформації та забезпеченням функціонування внутрішньої інформаційної системи.

У процесі роботи підприємство використовує комп'ютерну техніку, локальну мережу, серверне обладнання, програмне забезпечення та засоби мережевої взаємодії[16]. Працівники підприємства здійснюють обробку службових документів, працюють із електронною поштою, внутрішніми файлами та корпоративними ресурсами, що потребує забезпечення належного рівня інформаційної безпеки[3, ст. 24].

Організаційна структура підприємства включає адміністрацію, бухгалтерію, ІТ-відділ та працівників інших структурних підрозділів. Доступ до інформаційних ресурсів підприємства здійснюється відповідно до службових обов'язків працівників. Для роботи співробітників використовуються персональні комп'ютери, об'єднані в локальну мережу підприємства.

У ході проходження переддипломної практики було встановлено, що підприємство використовує локальну комп'ютерну мережу для забезпечення взаємодії між робочими станціями працівників, серверним обладнанням та мережевими пристроями. Для передачі інформації використовуються мережеві протоколи, корпоративна електронна пошта та внутрішні інформаційні ресурси підприємства.

Інформаційна інфраструктура підприємства включає:

- робочі станції працівників;

- серверне обладнання;
- мережеве обладнання;
- локальну мережу;
- засоби доступу до мережі Інтернет;
- програмне забезпечення для обробки та зберігання інформації.

Для забезпечення стабільної роботи інформаційної системи на підприємстві використовуються операційні системи сімейства Windows, офісне програмне забезпечення, мережеві служби та засоби адміністрування локальної мережі[12].

Під час проходження практики було проведено аналіз конфігурації робочих станцій, досліджено топологію локальної мережі, вивчено серверне обладнання та механізми розмежування прав доступу користувачів. Також було проаналізовано способи передачі інформації між працівниками підприємства та визначено основні канали можливого витоку даних.

У процесі дослідження встановлено, що найбільшу загрозу інформаційної безпеки підприємства становлять внутрішні загрози, пов'язані з несанкціонованим копіюванням файлів, передачею службової інформації через електронну пошту, використанням зовнішніх носіїв інформації та недостатнім контролем дій користувачів.

Оскільки працівники підприємства мають доступ до службової документації, електронних баз даних та внутрішніх інформаційних ресурсів, питання забезпечення захисту інформації є актуальним для підприємства[28]. Саме тому подальше дослідження буде спрямоване на аналіз внутрішніх загроз, каналів витоку інформації та розробку системи захисту інформації із використанням DLP-технологій.

2.2. Аналіз інформаційної інфраструктури

Інформаційна інфраструктура підприємства є основою забезпечення стабільної роботи всіх інформаційних процесів, пов'язаних із обробкою, передачею та зберіганням службової інформації. У ході проходження

переддипломної практики на підприємстві ТОВ «МАК-СЕРВІС» було проведено аналіз технічних та програмних компонентів інформаційної системи підприємства, досліджено особливості локальної мережі, робочих станцій, серверного обладнання та механізмів доступу до інформаційних ресурсів.

У процесі дослідження встановлено, що для забезпечення роботи підприємства використовуються персональні комп'ютери працівників, локальна комп'ютерна мережа, мережеве обладнання, серверне обладнання та програмні засоби для обробки службової інформації [16].

У ході проходження переддипломної практики було проведено аналіз робочих станцій працівників підприємства ТОВ «МАК-СЕРВІС». Під час дослідження перевірено конфігурацію комп'ютерів, параметри операційної системи, мережеві налаштування та встановлене програмне забезпечення.

На більшості робочих станцій використовувалась операційна система Windows 10 Pro. Для роботи працівників було встановлено:

- Microsoft Office;
- Google Chrome;
- Microsoft Edge;
- засоби роботи з електронною поштою;
- антивірусне програмне забезпечення Windows Defender.

У процесі аналізу було перевірено:

- IP-адреси пристроїв;
- параметри мережевих адаптерів;
- права локальних користувачів;
- налаштування спільного доступу до папок;
- наявність антивірусного захисту.

Під час дослідження встановлено, що частина користувачів мала доступ до спільних папок без обмеження прав на копіювання файлів. Також було виявлено використання USB-носіїв без контролю підключення пристроїв, що створює ризик копіювання службової інформації.

Вікно системних параметрів робочої станції підприємства наведено на рисунку 2.1.

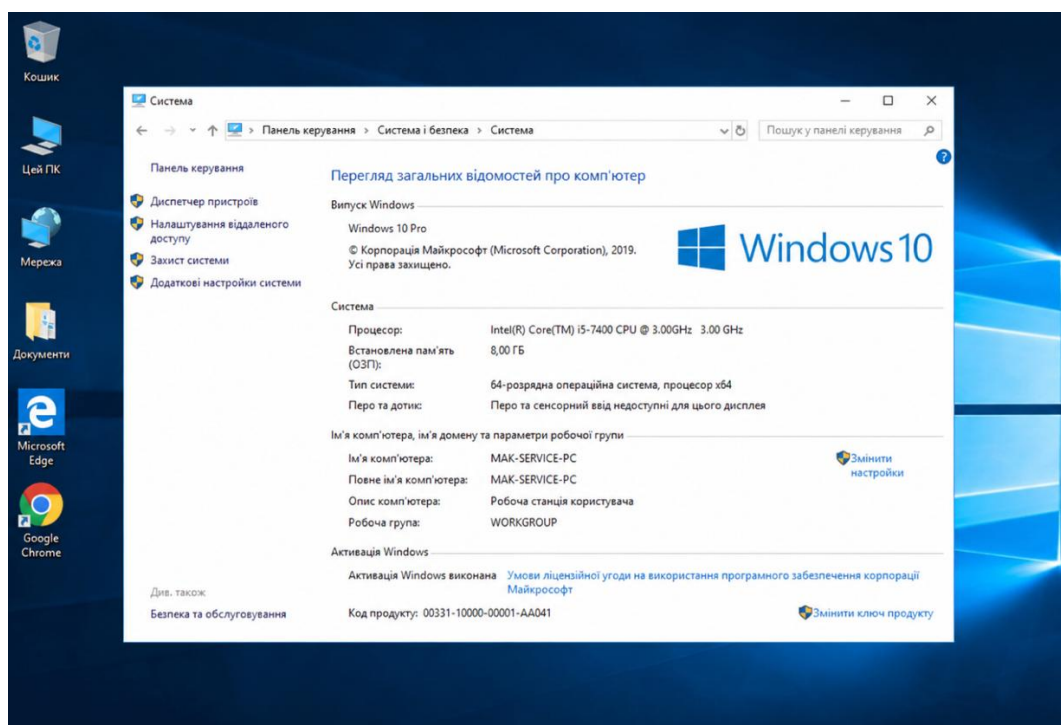


Рисунок 2.1 - Вікно системних параметрів робочої станції підприємства

Під час аналізу робочих станцій було встановлено, що користувачі мають доступ до локальних та мережевих ресурсів підприємства через облікові записи операційної системи Windows. Також було перевірено параметри мережевого підключення, IP-адресацію пристроїв та доступність мережевих ресурсів. Для дослідження мережевих параметрів використовувались стандартні мережеві утиліти операційної системи Windows, зокрема команда `ipconfig`, яка дозволяє визначити параметри мережевого адаптера та IP-конфігурацію пристрою[18].

Результат перевірки мережевих параметрів робочої станції за допомогою команди `ipconfig` наведено на рисунку 2.2.

```

C:\Users\User>ipconfig

Конфігурація IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::7c6e:1d3a:2f55:9baf%8
    IPv4-адреса. . . . . : 192.168.1.105
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 192.168.1.1

Адаптер бездротової локальної мережі Бездротова мережа:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::1d3d:8a65:3c8d:cb1e%12
    IPv4-адреса. . . . . : 192.168.1.106
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 192.168.1.1

Адаптер Ethernet VirtualBox Host-Only Network:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::a4e3:7b6f:6b22:7a6f%3
    IPv4-адреса. . . . . : 192.168.56.1
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 

C:\Users\User>

```

Рисунок 2.2 – Перевірка мережевих параметрів через ipconfig

Для забезпечення взаємодії між робочими станціями підприємства використовується локальна комп'ютерна мережа із доступом до мережі Інтернет через маршрутизатор та комутатор[19].

У ході дослідження локальної мережі було:

- визначено топологію мережі;
- перевірено мережеві підключення;
- досліджено параметри IP-адресації;
- проаналізовано роботу маршрутизатора та комутатора;
- виконано перевірку доступності пристроїв через команду ping.

У результаті аналізу встановлено, що всі робочі станції підприємства знаходяться в одній локальній мережі та мають доступ до спільних ресурсів сервера. Передача даних між пристроями здійснюється в межах єдиної локальної мережі без сегментації доступу, що підвищує ризик несанкціонованого доступу до службових файлів та поширення шкідливого програмного забезпечення.

У результаті аналізу також встановлено відсутність централізованого журналювання мережевої активності користувачів та контролю передачі файлів між робочими станціями.

Схему локальної мережі підприємства наведено на рисунку 2.3.

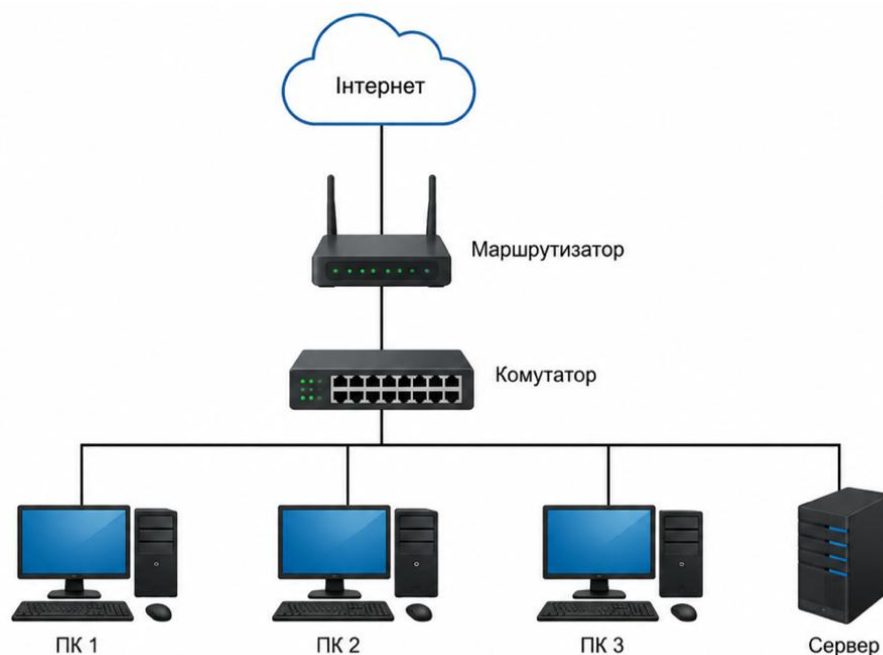
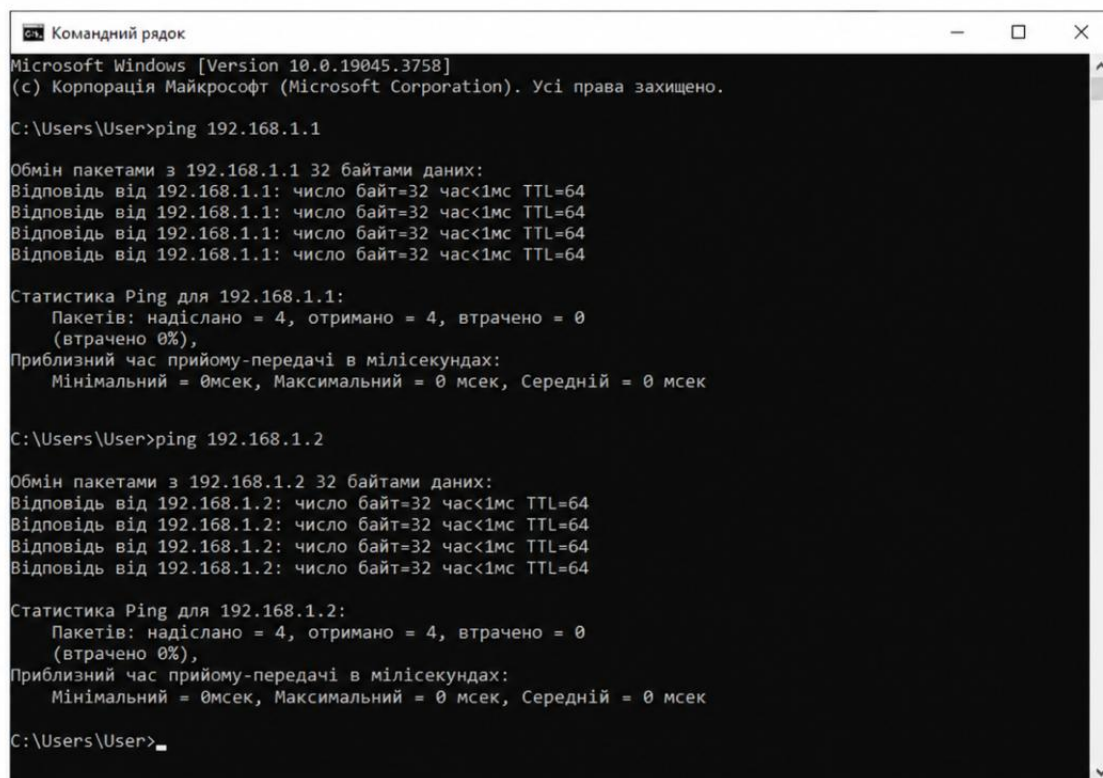


Рисунок 2.3 – Схема локальної мережі підприємства

Для перевірки працездатності локальної мережі та доступності мережевих пристроїв було використано мережеву утиліту ping. У ході аналізу здійснювалась перевірка з'єднання між робочими станціями та мережевими ресурсами підприємства. Результати перевірки підтвердили наявність активного мережевого підключення між пристроями локальної мережі.

Результат перевірки доступності мережевих пристроїв командою ping наведено на рисунку 2.4



```
Командний рядок
Microsoft Windows [Version 10.0.19045.3758]
(c) Корпорація Майкрософт (Microsoft Corporation). Усі права захищено.

C:\Users\User>ping 192.168.1.1

Обмін пакетами з 192.168.1.1 32 байтами даних:
Відповідь від 192.168.1.1: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.1: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.1: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.1: число байт=32 час<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетів: надіслано = 4, отримано = 4, втрачено = 0
    (втрачено 0%),
    Приблизний час прийому-передачі в мілісекундах:
        Мінімальний = 0мсек, Максимальний = 0 мсек, Середній = 0 мсек

C:\Users\User>ping 192.168.1.2

Обмін пакетами з 192.168.1.2 32 байтами даних:
Відповідь від 192.168.1.2: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.2: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.2: число байт=32 час<1мс TTL=64
Відповідь від 192.168.1.2: число байт=32 час<1мс TTL=64

Статистика Ping для 192.168.1.2:
    Пакетів: надіслано = 4, отримано = 4, втрачено = 0
    (втрачено 0%),
    Приблизний час прийому-передачі в мілісекундах:
        Мінімальний = 0мсек, Максимальний = 0 мсек, Середній = 0 мсек

C:\Users\User>
```

Рисунок 2.4 – Перевірка доступності пристроїв командою ping

Під час аналізу мережевих параметрів було перевірено IP-конфігурацію робочих станцій, параметри мережевих адаптерів та доступність мережевих ресурсів підприємства. Для цього використовувалась мережева утиліта ipconfig операційної системи Windows[16, ст. 211].

Результат аналізу мережевого підключення робочої станції наведено на рисунку 2.5.

```

Командний рядок
Microsoft Windows [Version 10.0.19045.3758]
(c) Корпорація Майкрософт (Microsoft Corporation). Усі права захищено.

C:\Users\User>ipconfig

Конфігурація IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::7c6e:1d3a:2f55:9baf%8
    IPv4-адреса. . . . . : 192.168.1.105
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 192.168.1.1

Адаптер бездротової локальної мережі Бездротова мережа:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::1d3d:8a65:3c8d:cb1e%12
    IPv4-адреса. . . . . : 192.168.1.106
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 192.168.1.1

Адаптер Ethernet VirtualBox Host-Only Network:

    DNS-суфікс підключення . . . . . : 
    Локальний IPv6-адрес . . . . . : fe80::a4e3:7b6f:6b22:7a6f%3
    IPv4-адреса. . . . . : 192.168.56.1
    Маска підмережі . . . . . : 255.255.255.0
    Основний шлюз. . . . . : 

C:\Users\User>

```

Рисунок 2.5 – Аналіз мережевого підключення

Під час проходження практики було проведено дослідження серверного обладнання підприємства, яке використовується для зберігання службових документів, організації спільного доступу до файлів та резервного копіювання інформації[12, ст. 38; 17, ст. 95].

У ході аналізу було досліджено:

- структуру серверних папок;
- права доступу користувачів;
- механізми авторизації;
- резервне копіювання даних;
- мережевий доступ до сервера.

У результаті дослідження встановлено, що сервер використовується як централізоване файлове сховище для працівників підприємства[20]. Доступ до окремих папок надається через локальну мережу.

Було виявлено, що частина службових файлів зберігається без шифрування та додаткового контролю копіювання інформації. Також не використовуються спеціалізовані засоби моніторингу передачі конфіденційних даних.

Структуру взаємодії серверного обладнання підприємства наведено на рисунку 2.6.

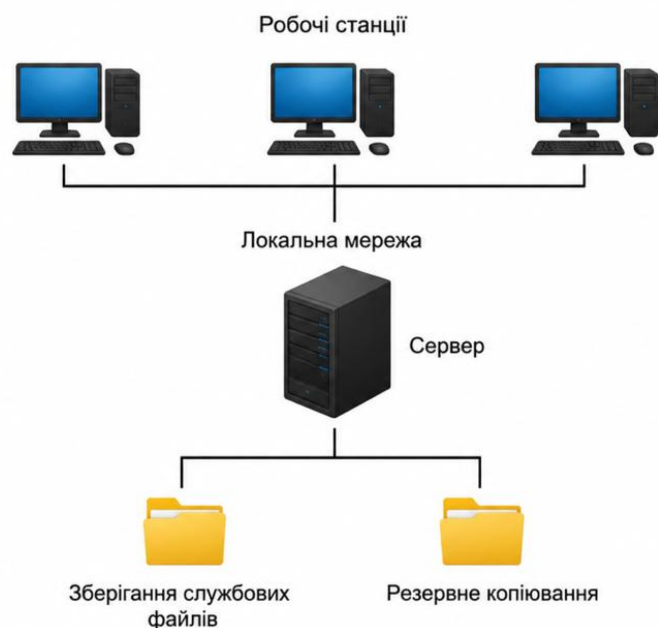


Рисунок 2.6 – Структура взаємодії серверного обладнання

Під час аналізу серверного обладнання було досліджено механізм надання доступу користувачам до спільних мережеских папок. Встановлено, що доступ до службових файлів здійснюється через локальну мережу підприємства відповідно до прав користувачів операційної системи. Аналіз також показав відсутність додаткового контролю копіювання файлів та моніторингу передачі конфіденційної інформації.

Приклад спільного доступу до серверних папок наведено на рисунку 2.7.

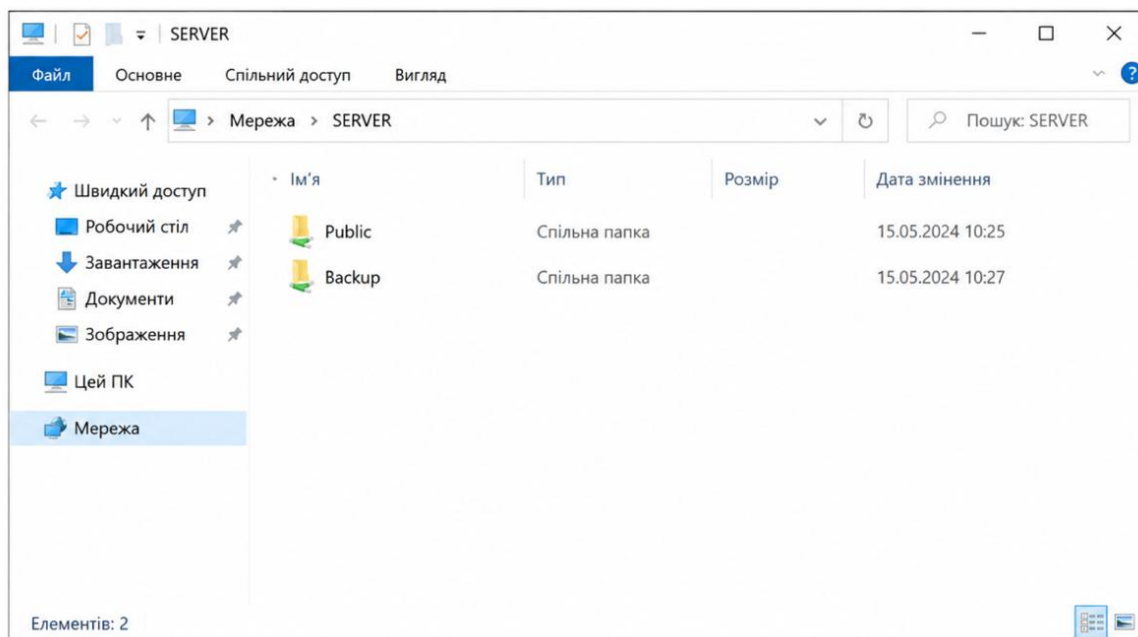


Рисунок 2.7 – Спільний доступ до серверних папок

У процесі дослідження було проведено аналіз програмного забезпечення та механізмів забезпечення інформаційної безпеки підприємства.

На робочих станціях використовувались:

- Microsoft Office;
- браузери Google Chrome та Microsoft Edge;
- засоби електронної пошти;
- Windows Defender.

Під час аналізу системи захисту інформації встановлено такі проблеми:

- відсутній контроль підключення USB-носіїв;
- не використовується DLP-система;
- відсутній централізований моніторинг передачі файлів;
- користувачі мають можливість копіювати файли на зовнішні носії;
- передача службових документів може здійснюватися через електронну пошту без додаткового контролю.

У результаті аналізу було визначено основні потенційні канали витоку інформації:

- USB-носії;
- електронна пошта;

- хмарні сервіси;
- локальна мережа (рис. 2.8).



Рисунок 2.8 – Основні канали можливого витоку інформації

Для оцінки рівня захищеності робочих станцій також було проведено аналіз встановленого програмного забезпечення. У ході дослідження перевірено перелік встановлених програм, засобів захисту інформації та системних компонентів операційної системи Windows (рис. 2.9).

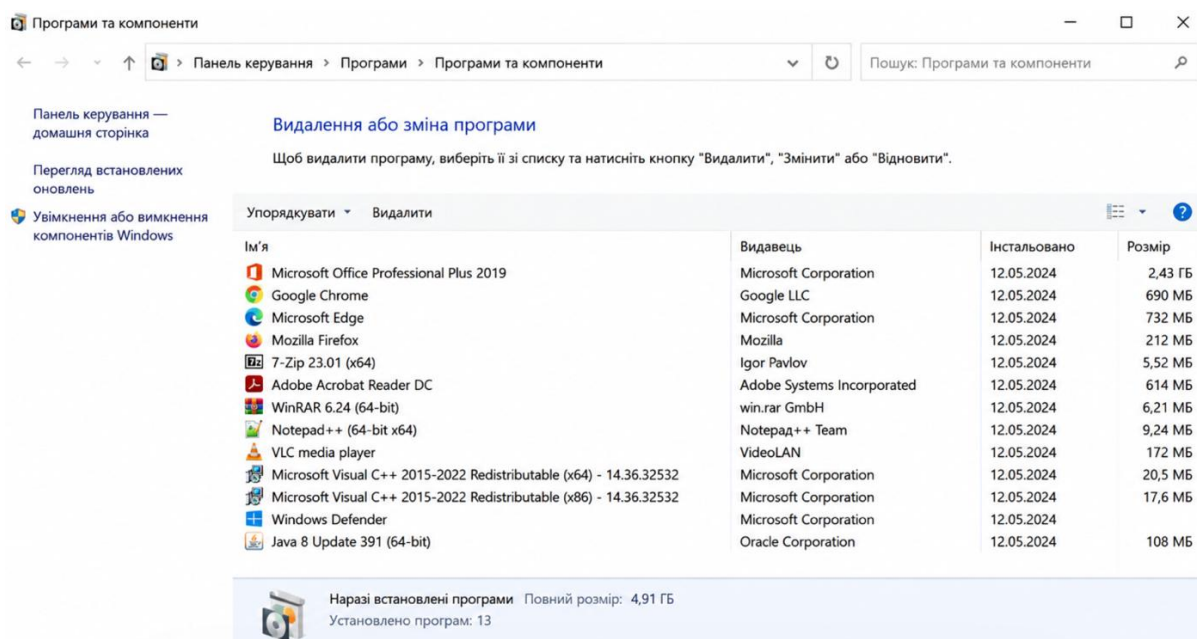


Рисунок 2.9 – Перевірка встановленого програмного забезпечення

Таким чином, у результаті аналізу інформаційної інфраструктури підприємства було досліджено структуру локальної мережі, робочі станції, серверне обладнання та програмне забезпечення підприємства. У ході дослідження визначено основні компоненти інформаційної системи, виявлено потенційні загрози інформаційній безпеці та встановлено необхідність впровадження DLP-технологій для контролю передачі інформації та запобігання витоку конфіденційних даних[27; 31;36].

2.3. Визначення інформаційних активів підприємства

Інформаційні активи підприємства є одним із основних елементів системи інформаційної безпеки, оскільки саме вони містять службову, конфіденційну та комерційно важливу інформацію, що потребує належного захисту від несанкціонованого доступу, втрати або витоку[3, ст. 47].

У процесі проходження переддипломної практики на підприємстві ТОВ «МАК-СЕРВІС» було проведено аналіз основних інформаційних активів підприємства, досліджено місця їх зберігання, способи обробки та рівень доступу користувачів до інформаційних ресурсів.

У результаті аналізу встановлено, що до основних інформаційних активів підприємства належать:

- службова документація;
- електронна пошта працівників;
- база клієнтів;
- договори та фінансова документація;
- облікові записи користувачів;
- файли локальної мережі;
- серверні папки та резервні копії даних.

Інформаційні активи підприємства зберігаються на робочих станціях користувачів, серверному обладнанні та в локальній мережі підприємства. Частина службової інформації передається через електронну пошту та зовнішні носії інформації, що створює потенційні ризики витоку конфіденційних даних[20, ст. 96].

Основні інформаційні активи підприємства наведено на рисунку 2.10.



Рисунок 2.10 – Основні інформаційні активи підприємства

У ході дослідження також було визначено основні місця зберігання інформаційних активів. Встановлено, що найбільший обсяг службових даних

зберігається на сервері підприємства та у спільних мережових папках. Доступ до інформації здійснюється через локальну мережу відповідно до прав користувачів операційної системи (рис.2.11).



Рисунок 2.11 – Місця зберігання інформаційних активів

Під час аналізу доступу користувачів до інформаційних ресурсів встановлено, що працівники мають доступ до окремих службових папок, електронної пошти та внутрішніх документів підприємства. При цьому частина інформації може копіюватися на зовнішні носії або передаватися через електронну пошту без додаткового контролю передачі даних.

У результаті дослідження визначено основні ризики для інформаційних активів підприємства:

- несанкціоноване копіювання файлів;
- передача конфіденційної інформації через електронну пошту;
- використання USB-носіїв;
- видалення або пошкодження службових даних;
- несанкціонований доступ до мережових ресурсів.

Для мінімізації зазначених ризиків було проаналізовано існуючий розподіл прав доступу користувачів до інформаційних ресурсів підприємства. Результати аналізу наведено на рисунку 2.12.



Рисунок 2.12 – Розподіл доступу користувачів до інформаційних ресурсів

Як показано на рисунку 2.12, на підприємстві використовується розподіл прав доступу до інформаційних ресурсів залежно від посадових обов'язків працівників. Найширші повноваження має адміністратор системи, який здійснює управління користувачами та налаштування безпеки. Керівництво має доступ до більшості інформаційних ресурсів підприємства, тоді як працівники відділів і бухгалтерії отримують доступ лише до інформації, необхідної для виконання своїх функціональних обов'язків. Для гостьових користувачів передбачено обмежений доступ до окремих ресурсів. Такий підхід дозволяє частково знизити ризик несанкціонованого доступу до інформації, однак не забезпечує контролю копіювання файлів та передачі конфіденційних даних за межі підприємства.

2.4. Аналіз внутрішніх загроз витоку інформації

У процесі дослідження інформаційної інфраструктури підприємства було проведено аналіз внутрішніх загроз витоку конфіденційної інформації та визначено основні фактори, що можуть негативно впливати на рівень інформаційної безпеки підприємства. Встановлено, що найбільшу небезпеку для інформаційних ресурсів організації становлять внутрішні порушники, які мають доступ до локальної мережі, службових документів та серверних ресурсів [4, с. 214; 13, с. 167].

У ході аналізу визначено, що основними внутрішніми загрозами для підприємства є:

- копіювання службових файлів на USB-носії;
- передача конфіденційної інформації через електронну пошту;
- використання хмарних сервісів для зберігання службових документів;
- несанкціонований доступ до серверних папок;
- відсутність централізованого контролю передачі файлів;
- випадкове або навмисне видалення службової інформації [18, с. 143; 20, с. 96].

Для наочного відображення результатів проведеного аналізу внутрішніх загроз побудовано схему основних ризиків витоку інформації на підприємстві. Схему внутрішніх загроз інформаційній безпеці підприємства наведено на рисунку 2.13.



Рисунок 2.13 – Основні внутрішні загрози інформаційній безпеці підприємства

Під час дослідження встановлено, що працівники підприємства мають можливість використовувати зовнішні носії інформації та передавати файли через електронну пошту без додаткового контролю передачі даних. Відсутність DLP-системи та механізмів моніторингу дій користувачів підвищує ризик витоку конфіденційної інформації та несанкціонованого копіювання службових документів [27; 31; 38].

Також було визначено основні канали можливого витоку інформації на підприємстві:

- USB-носії;
- електронна пошта;
- локальна мережа;
- хмарні сервіси;
- месенджери та веб-сервіси [36; 40].

Канали можливого витоку інформації наведено на рисунку 2.14.

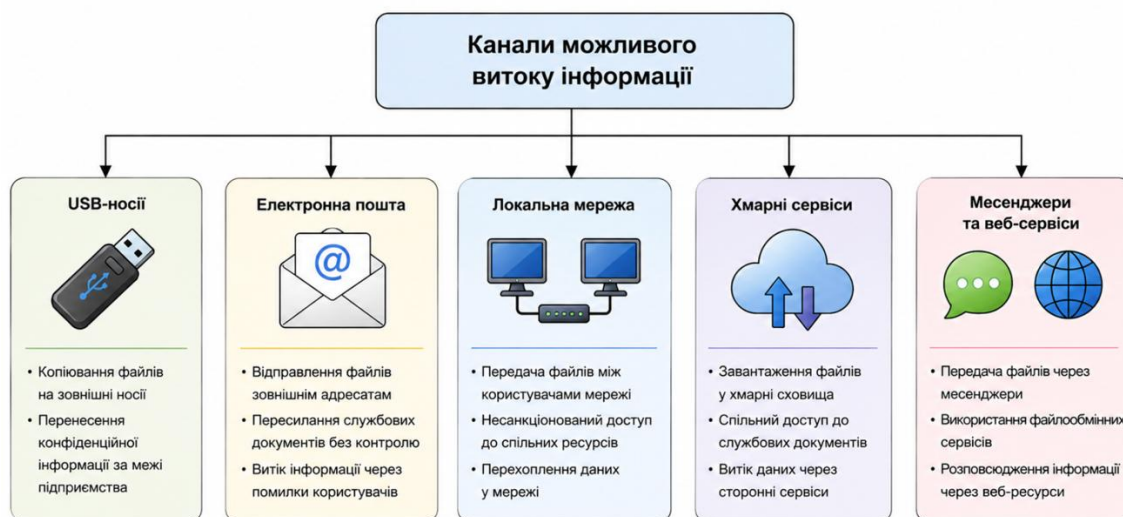


Рисунок 2.14 – Канали можливого витоку інформації на підприємстві

У результаті проведеного аналізу встановлено, що на підприємстві відсутній централізований контроль передачі конфіденційної інформації між користувачами та зовнішніми ресурсами. Також не використовуються механізми автоматичного блокування передачі службових файлів через зовнішні носії або електронну пошту, що створює значні ризики порушення інформаційної безпеки [28;32].

Для оцінки рівня небезпеки внутрішніх загроз було проведено аналіз потенційних ризиків витоку інформації (табл. 2.1).

Оцінка ризиків внутрішніх загроз витоку інформації

Таблиця 2.1

Внутрішня загроза	Рівень ризику
Копіювання файлів на USB-носії	Високий
Передача файлів через електронну пошту	Високий
Використання хмарних сервісів	Середній
Несанкціонований доступ до серверних папок	Високий
Видалення службових документів	Середній

Таким чином, у результаті аналізу внутрішніх загроз витоку інформації було визначено основні потенційні джерела порушення інформаційної безпеки підприємства та встановлено недостатній рівень контролю передачі конфіденційних даних. Проведене дослідження підтвердило необхідність впровадження DLP-системи для моніторингу дій користувачів, контролю передачі файлів та запобігання витоку службової інформації.

2.5. Аналіз системи контролю доступу

У процесі дослідження інформаційної інфраструктури підприємства було проведено аналіз системи контролю доступу до інформаційних ресурсів, серверного обладнання та службових документів. Встановлено, що контроль доступу є одним із ключових елементів забезпечення інформаційної безпеки підприємства, оскільки дозволяє обмежити доступ користувачів до конфіденційної інформації відповідно до їх посадових обов'язків [12, с. 148; 13, с. 203].

У ході аналізу було досліджено:

- механізми авторизації користувачів;
- розмежування прав доступу;
- доступ до серверних папок;
- використання облікових записів користувачів;
- контроль доступу до мережевих ресурсів;
- механізми захисту службових даних [18, с. 176; 22, с. 154].

Встановлено, що доступ до робочих станцій підприємства здійснюється за допомогою облікових записів операційної системи Windows. Користувачі мають різний рівень доступу до інформаційних ресурсів залежно від виконуваних функцій та посадових обов'язків. Адміністратор системи має повний доступ до серверного обладнання, мережевих ресурсів та системних налаштувань, тоді як працівники підприємства мають доступ лише до окремих службових папок та документів.

Під час дослідження встановлено, що на підприємстві використовується базове розмежування прав доступу до мережесих ресурсів, проте відсутній централізований моніторинг дій користувачів та контроль передачі конфіденційної інформації. Також не використовуються механізми багатофакторної автентифікації та додаткового контролю доступу до критично важливих ресурсів [28; 29; 32].

У результаті аналізу було визначено основні недоліки системи контролю доступу:

- відсутність DLP-системи;
- недостатній контроль копіювання службових файлів;
- відсутність моніторингу дій користувачів;
- можливість використання зовнішніх носіїв інформації;
- відсутність журналювання передачі файлів;
- недостатній контроль доступу до серверних ресурсів [27; 31; 36].

Проведений аналіз показав, що існуюча система контролю доступу забезпечує базовий рівень захисту інформації, проте не дозволяє ефективно контролювати передачу конфіденційних даних та своєчасно виявляти потенційні загрози витоку інформації. Це створює необхідність впровадження додаткових механізмів захисту та використання DLP-технологій для моніторингу дій користувачів і контролю передачі інформації в інформаційній системі підприємства.

2.6. Висновки до розділу 2

У другому розділі дипломної роботи було проведено аналіз інформаційної системи підприємства та досліджено основні загрози витоку інформації в інформаційній інфраструктурі ТОВ «МАК-СЕРВІС». У ході дослідження проаналізовано структуру локальної мережі, серверне обладнання, програмне забезпечення та механізми доступу користувачів до інформаційних ресурсів підприємства.

У результаті аналізу було визначено основні інформаційні активи підприємства, місця їх зберігання та канали передачі службової інформації. Встановлено, що передача конфіденційних даних може здійснюватися через електронну пошту, USB-носії, локальну мережу та хмарні сервіси.

Під час дослідження внутрішніх загроз витоку інформації виявлено низку проблем інформаційної безпеки, зокрема відсутність централізованого контролю передачі файлів, моніторингу дій користувачів та механізмів запобігання несанкціонованому копіюванню службових даних. Також встановлено недостатній рівень контролю доступу до інформаційних ресурсів підприємства.

Проведений аналіз підтвердив необхідність впровадження DLP-системи для контролю передачі конфіденційної інформації, моніторингу дій користувачів та підвищення рівня захисту інформаційних ресурсів підприємства від внутрішніх загроз витоку інформації.

РОЗДІЛ 3

РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ DLP-ТЕХНОЛОГІЇ

3.1. Побудова моделі внутрішнього порушника

У процесі розробки системи захисту інформації на основі DLP-технологій важливим етапом є побудова моделі внутрішнього порушника. Така модель дозволяє визначити потенційні джерела загроз інформаційній безпеці підприємства, оцінити їх можливості та сформулювати ефективні заходи протидії витоку конфіденційної інформації.

На основі результатів аналізу інформаційної інфраструктури ТОВ «МАКСЕРВІС», проведеного в другому розділі роботи, встановлено, що основну небезпеку для інформаційних ресурсів підприємства становлять працівники, які мають законний доступ до службової інформації, локальної мережі та серверних ресурсів.

Під внутрішнім порушником у даній роботі розуміється працівник підприємства або інша особа, яка має авторизований доступ до інформаційної системи та може навмисно або ненавмисно здійснити дії, що призведуть до порушення конфіденційності, цілісності або доступності інформації [13, с. 204; 20, с. 97].

З урахуванням структури підприємства було виділено такі категорії внутрішніх порушників:

- звичайний користувач (співробітник відділу);
- працівник бухгалтерії;
- керівник структурного підрозділу;
- системний адміністратор;
- звільнений або незадоволений працівник.

Найбільший рівень потенційної небезпеки становить системний адміністратор, оскільки має розширені права доступу до серверного обладнання, мережевих ресурсів та облікових записів користувачів. Водночас найбільш імовірним джерелом витoku інформації є звичайні працівники підприємства, які щоденно працюють із документами, електронною поштою та мережевими ресурсами.

Основними можливостями внутрішнього порушника можуть бути:

- копіювання службових документів на USB-носії;
- передача файлів через електронну пошту;
- використання хмарних сервісів для збереження інформації;
- передача даних через месенджери;
- видалення або зміна службових документів;
- несанкціоноване використання облікових записів інших користувачів.

На підставі проведеного аналізу сформовано модель внутрішнього порушника підприємства, яка наведена на рисунку 3.1.



Рисунок 3.1 – Модель внутрішнього порушника ТОВ «МАК-СЕРВІС»

Таким чином, побудована модель внутрішнього порушника дозволила визначити основні джерела внутрішніх загроз та сформувавши вимоги до майбутньої DLP-системи, яка повинна забезпечувати контроль дій користувачів, моніторинг передачі файлів та запобігання витоку конфіденційної інформації.

3.2. Впровадження журналювання дій користувачів

У результаті аналізу інформаційної інфраструктури ТОВ «МАК-СЕРВІС» було встановлено відсутність централізованого контролю дій користувачів та механізмів аудиту подій інформаційної безпеки. Це ускладнює виявлення несанкціонованого доступу до інформаційних ресурсів, фактів копіювання службових документів та передачі конфіденційної інформації стороннім особам.

Одним із ефективних засобів підвищення рівня інформаційної безпеки є впровадження системи журналювання подій, яка забезпечує фіксацію дій користувачів у локальній мережі та інформаційній системі підприємства [13, с. 246; 20, с. 142].

Для підприємства ТОВ «МАК-СЕРВІС» запропоновано впровадити аудит подій інформаційної безпеки із використанням вбудованих механізмів операційної системи Windows. Запропоноване рішення дозволить здійснювати контроль доступу до інформаційних ресурсів, реєструвати дії користувачів та своєчасно виявляти потенційні порушення політики інформаційної безпеки [18, с. 203; 32].

До основних подій, що підлягають журналюванню, віднесено:

- авторизацію користувачів у системі;
- невдалі спроби входу;
- доступ до серверних папок та службових документів;
- створення, зміну та видалення файлів;
- копіювання інформації на USB-носії;
- передачу файлів через електронну пошту;
- зміну прав доступу користувачів.

Основні події журналювання та їх призначення наведено в таблиці 3.1.

Події журналювання інформаційної системи

Таблиця 3.1

Подія	Мета контролю
Авторизація користувача	Контроль входу до системи
Невдала авторизація	Виявлення спроб злому
Доступ до файлів	Контроль роботи з документами
Копіювання на USB	Виявлення можливого витоку
Надсилення електронної пошти	Контроль передачі інформації
Зміна прав доступу	Контроль адміністративних дій

Під час подальшого впровадження DLP-системи журнали подій можуть використовуватися для автоматичного виявлення підозрілих дій користувачів, формування повідомлень про потенційні інциденти інформаційної безпеки та блокування несанкціонованої передачі конфіденційної інформації [27; 31; 36].

Запропонований механізм журналювання забезпечить простежуваність дій користувачів, підвищить ефективність контролю за використанням інформаційних ресурсів та створить додатковий рівень захисту від внутрішніх загроз витоку інформації. Це також сприятиме підвищенню ефективності роботи майбутньої DLP-системи, яка буде впроваджена на підприємстві.

3.3. Обґрунтування вибору DLP - системи

У результаті аналізу інформаційної інфраструктури ТОВ «МАК-SERVIS», проведеного в другому розділі роботи, було встановлено наявність низки проблем у сфері захисту конфіденційної інформації. Зокрема, виявлено відсутність централізованого контролю передачі файлів, моніторингу дій користувачів, контролю зовнішніх носіїв інформації та механізмів запобігання витоку службових даних через електронну пошту й мережеві сервіси.

Для усунення виявлених недоліків запропоновано впровадження DLP-системи (Data Loss Prevention), призначеної для контролю інформаційних потоків та запобігання несанкціонованому витоку конфіденційної інформації [27; 31; 36].

Під час вибору програмного рішення було сформовано основні вимоги до DLP-системи для ТОВ «МАК-СЕРВІС»:

- контроль використання USB-носіїв;
- моніторинг електронної пошти;
- контроль передачі файлів через локальну мережу;
- журналювання дій користувачів;
- формування звітів про інциденти інформаційної безпеки;
- централізоване адміністрування;
- можливість інтеграції з існуючою інформаційною інфраструктурою підприємства [13, с. 246; 20, с. 142].

Для вибору найбільш доцільного рішення було проведено порівняльний аналіз трьох сучасних DLP-систем: SearchInform DLP, Falcongaze SecureTower та Microsoft Purview DLP. Порівняння здійснювалося за критеріями функціональності, можливостей контролю каналів витоку інформації та особливостей впровадження.

Основні результати порівняння наведено в таблиці 3.2.

Порівняння DLP-систем

Таблиця 3.2

Критерій	SearchInform DLP	Falcongaze SecureTower	Microsoft Purview DLP
Контроль USB-носіїв	Так	Так	Так
Контроль електронної пошти	Так	Так	Так
Контроль мережевого трафіку	Так	Так	Частково

продовження табл. 3.2

Моніторинг дій користувачів	Так	Так	Обмежено
Журналювання подій	Так	Так	Так
Формування звітів	Так	Так	Так
DLP-аналітика та розслідування інцидентів	Так	Так	Частково
Контроль хмарних сервісів	Так	Так	Так
Підтримка локальної інфраструктури	Так	Так	Частково
Складність впровадження	Середня	Висока	Середня
Вартість впровадження	Середня	Висока	Висока
Доцільність для ТОВ «МАК-SERBIC»	Висока	Середня	Середня

Проведений аналіз показав, що система Microsoft Purview DLP орієнтована переважно на використання хмарних сервісів Microsoft 365 та потребує відповідної ліцензійної інфраструктури[31]. З огляду на те, що інформаційна система ТОВ «МАК-SERBIC» побудована переважно на локальній мережі та власному серверному обладнанні, використання цього рішення є менш доцільним.

Система Falcongaze SecureTower забезпечує широкий набір інструментів контролю інформаційних потоків та моніторингу дій користувачів, проте характеризується більш складним адмініструванням і потребує значних ресурсів для впровадження та супроводу[40].

За результатами порівняльного аналізу найбільш доцільним рішенням для ТОВ «МАК-СЕРВІС» визначено SearchInform DLP. Система забезпечує контроль усіх основних каналів витоку інформації, включаючи USB-носії, електронну пошту, локальну мережу та хмарні сервіси. Крім того, SearchInform DLP підтримує функції моніторингу дій користувачів, аналізу подій інформаційної безпеки та формування звітності щодо інцидентів [27; 38].

Для підприємства пропонується впровадження SearchInform DLP із використанням централізованого сервера керування та агентів моніторингу, встановлених на робочих станціях користувачів. Такий підхід дозволить забезпечити безперервний контроль передачі інформації, виявляти спроби несанкціонованого копіювання службових документів та своєчасно реагувати на потенційні інциденти інформаційної безпеки.

Запропоновану схему впровадження SearchInform DLP у ТОВ «МАК-СЕРВІС» наведено на рисунку 3.2.

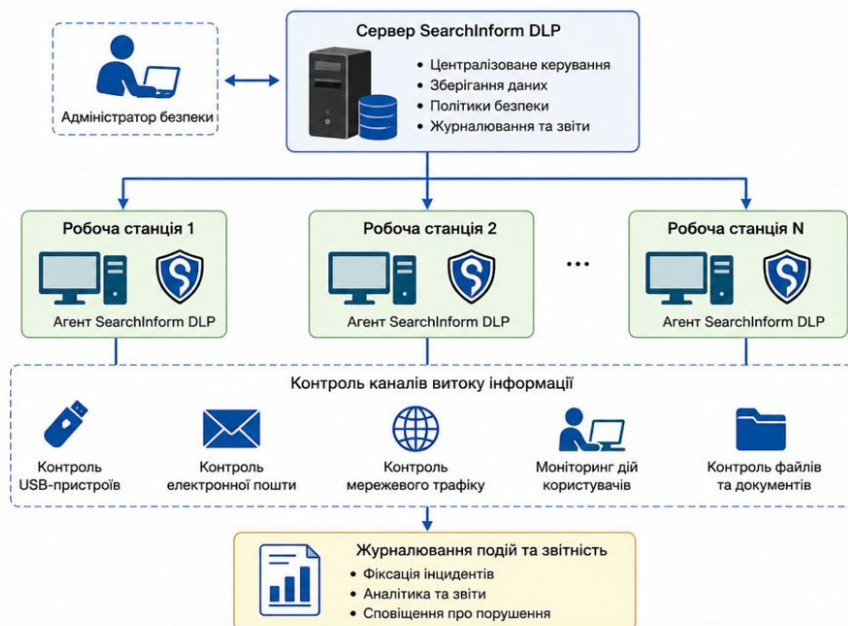


Рисунок 3.2 – Схема впровадження SearchInform DLP у ТОВ «МАК-СЕРВІС»

Як показано на рисунку 3.2, система SearchInform DLP передбачає встановлення центрального сервера керування та агентів моніторингу на робочих

станціях користувачів. Така архітектура забезпечує централізований контроль передачі інформації, використання зовнішніх носіїв, електронної пошти та мережевих ресурсів, що дозволяє своєчасно виявляти та блокувати потенційні спроби витоку конфіденційних даних [27; 38].

Таким чином, за результатами проведеного аналізу для побудови системи захисту інформації ТОВ «МАК-СЕРВІС» обрано SearchInform DLP. Використання даного рішення дозволить реалізувати контроль основних каналів витоку інформації, підвищити рівень моніторингу дій користувачів та забезпечити ефективний захист конфіденційних даних підприємства від внутрішніх загроз.

3.4. Розробка системи захисту на основі SearchInform DLP

У результаті аналізу інформаційної інфраструктури ТОВ «МАК-СЕРВІС», проведеного у другому розділі роботи, було встановлено наявність низки загроз інформаційній безпеці підприємства. Зокрема, виявлено відсутність централізованого контролю передачі файлів, моніторингу дій користувачів, контролю зовнішніх носіїв інформації та засобів запобігання витоку конфіденційних даних через електронну пошту й мережеві сервіси. Проведений аналіз показав необхідність створення комплексної системи захисту інформації, здатної забезпечити контроль основних каналів витоку даних та своєчасне виявлення інцидентів інформаційної безпеки.

З метою усунення виявлених недоліків було розроблено систему захисту інформації на основі SearchInform DLP. Дана система призначена для контролю інформаційних потоків, моніторингу дій користувачів та запобігання несанкціонованому розповсюдженню конфіденційної інформації в межах інформаційної системи підприємства [27; 38].

Під час проходження переддипломної практики було встановлено, що інформаційна інфраструктура ТОВ «МАК-СЕРВІС» складається із серверного обладнання, локальної мережі та робочих станцій співробітників. Передача службової інформації здійснюється через мережеві папки, електронну пошту,

зовнішні носії інформації та мережеві сервіси. При цьому відсутність спеціалізованих засобів контролю створює ризики несанкціонованого копіювання та передачі службових документів.

У межах розробленої системи захисту передбачається встановлення центрального сервера SearchInform DLP та програмних агентів на всіх робочих станціях працівників підприємства. Сервер виконує функції централізованого керування, збору інформації про події безпеки та формування звітності, тоді як агенти здійснюють контроль дій користувачів у режимі реального часу.

До основних інформаційних ресурсів, які підлягають захисту в межах розробленої системи, належать:

- службова документація підприємства;
- договори з клієнтами та контрагентами;
- фінансова документація;
- база даних клієнтів;
- електронна пошта співробітників;
- резервні копії інформації;
- документи, що передаються локальною мережею.

Для забезпечення комплексного захисту інформації до складу системи включено декілька функціональних модулів SearchInform DLP. Кожен модуль відповідає за контроль окремого каналу передачі інформації та взаємодіє з центральним сервером керування.

До складу розробленої системи входять:

- сервер SearchInform DLP;
- агенти моніторингу на робочих станціях;
- модуль контролю USB-пристроїв;
- модуль контролю електронної пошти;
- модуль контролю мережевого трафіку;
- модуль моніторингу дій користувачів;
- модуль журналювання подій;
- модуль формування звітів та сповіщень [27; 31].

Запропоновану архітектуру системи захисту інформації наведено на рисунку 3.3.

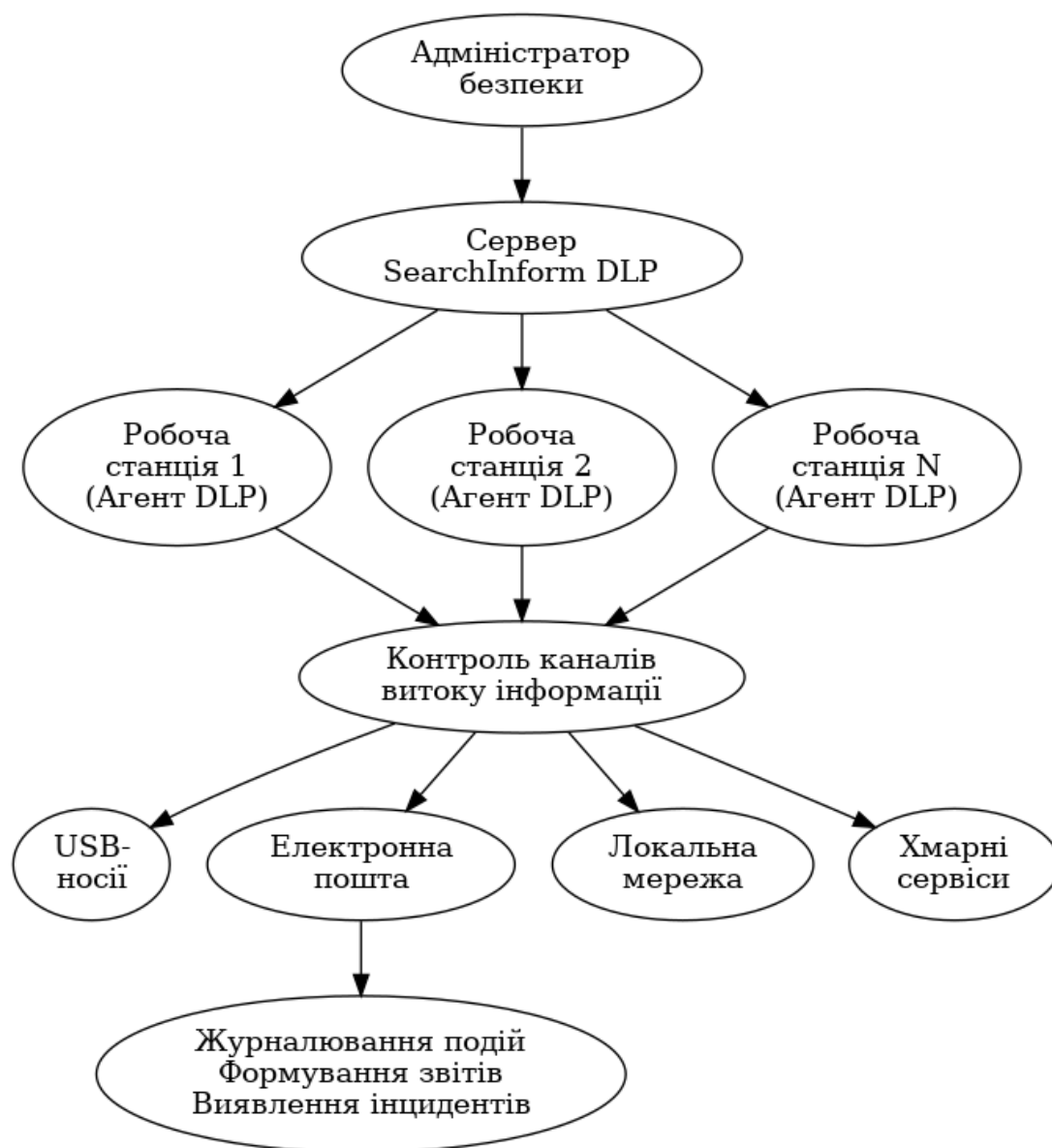


Рисунок 3.3 – Архітектура системи захисту інформації на основі SearchInform DLP

Як показано на рисунку 3.3, усі робочі станції підприємства підключаються до центрального сервера SearchInform DLP через програмні агенти. Агенти здійснюють збір інформації про дії користувачів, контроль передачі файлів, використання зовнішніх носіїв та роботу з конфіденційними документами. Отримані дані передаються на сервер для подальшого аналізу та обробки.

У процесі роботи агенти здійснюють контроль таких подій:

- підключення USB-пристроїв;
- копіювання службових документів;
- передача файлів через електронну пошту;
- використання хмарних сервісів;
- передача інформації через локальну мережу;
- спроби доступу до конфіденційних даних.

У разі виявлення дій, що суперечать встановленим політикам безпеки, система автоматично формує повідомлення для адміністратора безпеки та реєструє інцидент у журналі подій. Це дозволяє своєчасно реагувати на потенційні загрози та запобігати витоку конфіденційної інформації [32; 36].

Основні функції розробленої системи наведено в таблиці 3.3.

Основні функції розробленої системи захисту

Таблиця 3.3

Компонент системи	Призначення
Сервер SearchInform DLP	Централізоване керування системою
Агент моніторингу	Контроль дій користувачів
Контроль USB-пристроїв	Запобігання копіюванню інформації
Контроль електронної пошти	Аналіз повідомлень та вкладень
Контроль мережевого трафіку	Моніторинг передачі файлів
Журналювання подій	Реєстрація подій безпеки
Формування звітності	Підготовка звітів та сповіщень

Розроблена система забезпечує багаторівневий захист інформації. Перший рівень реалізує контроль доступу користувачів до інформаційних ресурсів підприємства. Другий рівень забезпечує контроль каналів передачі інформації та моніторинг потенційних каналів витоку даних. Третій рівень виконує аналіз подій

інформаційної безпеки, журналювання інцидентів та формування повідомлень для відповідальних осіб.

Таким чином, у межах даного підрозділу було розроблено систему захисту інформації на основі SearchInform DLP для ТОВ «МАК-СЕРВІС». Запропоноване рішення враховує особливості інформаційної інфраструктури підприємства, забезпечує контроль основних каналів витоку інформації та створює основу для реалізації заходів захисту, що будуть розглянуті в наступному підрозділі.

3.5. Реалізація заходів захисту

Після розробки архітектури системи захисту інформації на основі SearchInform DLP було виконано проєктування комплексу заходів захисту, спрямованих на усунення виявлених недоліків системи інформаційної безпеки ТОВ «МАК-СЕРВІС». Розроблені заходи базуються на результатах аналізу інформаційної інфраструктури підприємства та враховують основні канали можливого витоку інформації, визначені у другому розділі роботи.

У ході дослідження було встановлено, що найбільший ризик для інформаційної безпеки підприємства становлять несанкціоноване копіювання службових документів на зовнішні носії інформації, передача конфіденційних даних через електронну пошту, використання хмарних сервісів для зберігання службової інформації та відсутність централізованого контролю дій користувачів. Для усунення зазначених недоліків було розроблено набір політик безпеки, які пропонується реалізувати в межах SearchInform DLP [27; 38].

Першим етапом реалізації заходів захисту є розробка політики контролю зовнішніх носіїв інформації. Для підприємства запропоновано використання механізму контролю USB-пристроїв, який дозволяє блокувати підключення незареєстрованих носіїв інформації. Передбачається, що використання зовнішніх накопичувачів буде дозволене лише для корпоративних пристроїв, внесених до переліку дозволених носіїв.

Схему реалізації контролю USB-пристроїв наведено на рисунку 3.4.

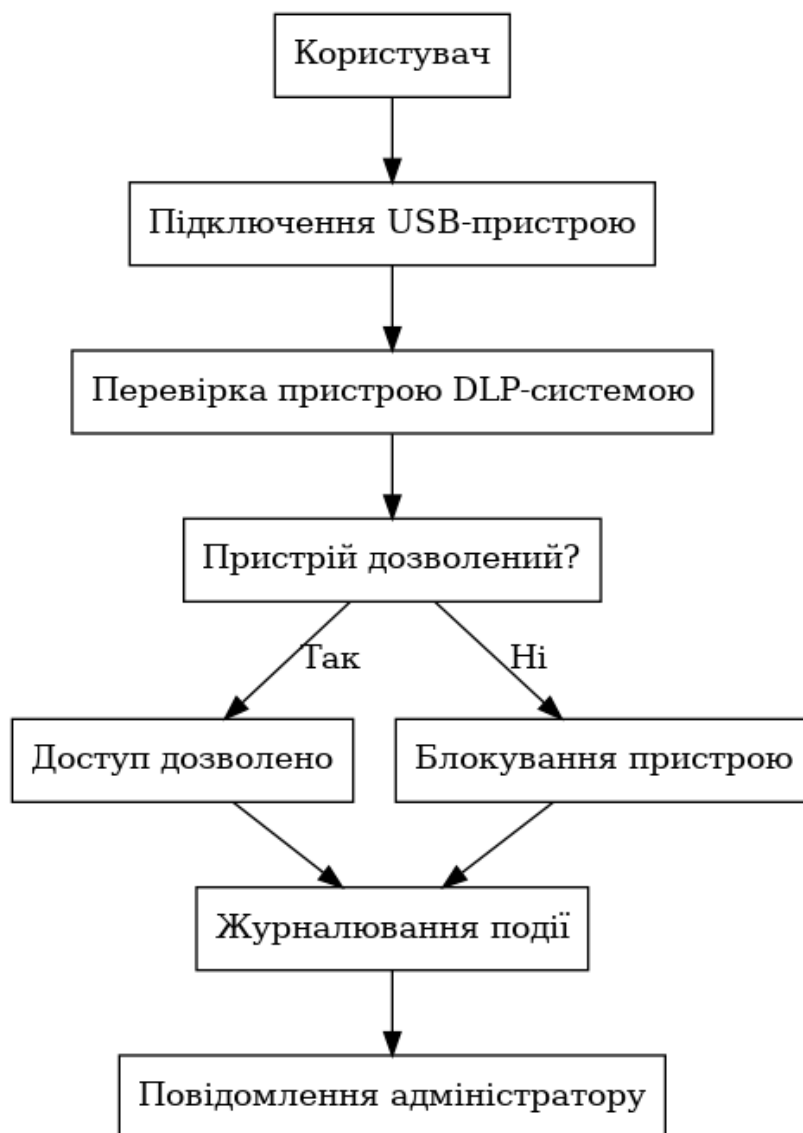


Рисунок 3.4 – Схема контролю USB-пристроїв у SearchInform DLP

Як показано на рисунку 3.4, після підключення зовнішнього носія система виконує перевірку його належності до переліку дозволених пристроїв. Якщо пристрій відсутній у списку дозволених, доступ до нього автоматично блокується, а інформація про подію реєструється в журналі безпеки.

Наступним етапом є реалізація політики контролю електронної пошти. З метою запобігання витоку конфіденційної інформації через електронні повідомлення було розроблено правила перевірки вкладень та текстового вмісту повідомлень. Система повинна здійснювати аналіз файлів, що передаються через електронну пошту, а також виконувати пошук визначених ключових слів.

Основні правила контролю електронної пошти наведено в таблиці 3.4.

Правила контролю електронної пошти

Таблиця 3.4

Тип файлу	Дія системи
DOCX	Аналіз вмісту
XLSX	Аналіз вмісту
PDF	Аналіз вмісту
ZIP	Додаткова перевірка
RAR	Додаткова перевірка

Для підвищення ефективності контролю передачі інформації було сформовано перелік ключових слів та категорій документів, які підлягають додатковому моніторингу. До таких категорій належать договори, фінансова документація, база клієнтів та службова документація підприємства.

Перелік ключових слів для виявлення конфіденційної інформації наведено в таблиці 3.5.

Ключові слова для виявлення конфіденційної інформації

Таблиця 3.5

Категорія документів	Ключові слова
Договори	договір, контракт, угода
Фінансова документація	рахунок, платіж, фінансовий звіт
Клієнтська база	клієнт, замовник, контактні дані
Службова документація	конфіденційно, службова інформація

Окремим напрямом реалізації заходів захисту є впровадження централізованого журналювання подій інформаційної безпеки. Для цього передбачається реєстрація всіх дій користувачів, пов'язаних із доступом до конфіденційної інформації, копіюванням файлів, використанням зовнішніх носіїв та передачею документів через мережеві сервіси. Отримані журнали можуть використовуватися для розслідування інцидентів інформаційної безпеки та аналізу дій користувачів [32; 36].

У межах розробленої системи захисту також передбачено механізм автоматичного сповіщення адміністратора безпеки про виявлені порушення політик безпеки. У разі спроби копіювання конфіденційного документа на зовнішній носій або передачі службового файлу через електронну пошту система формує повідомлення та реєструє відповідний інцидент.

Загальну схему реалізації політик безпеки в межах SearchInform DLP наведено на рисунку 3.5.

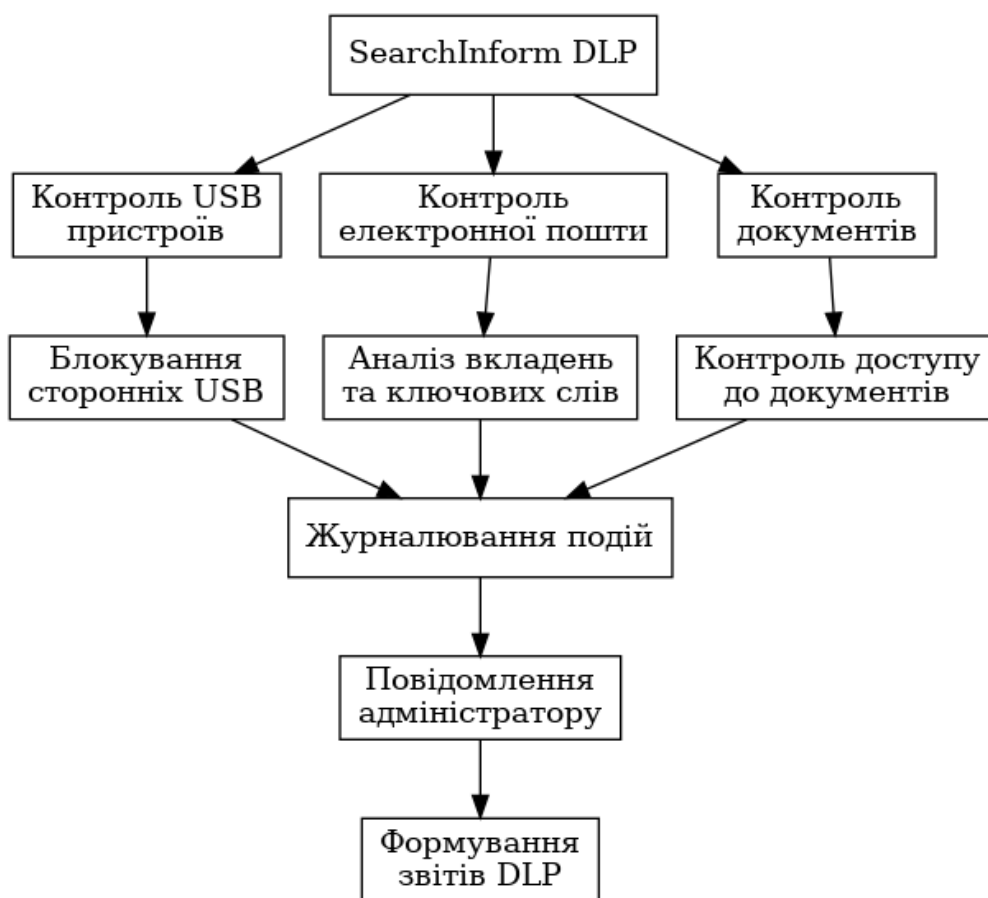


Рисунок 3.5 – Реалізація політик безпеки SearchInform DLP

Як показано на рисунку 3.5, усі інформаційні потоки проходять через механізми контролю SearchInform DLP. Система здійснює аналіз дій користувачів, контролює використання зовнішніх носіїв, перевіряє передачу файлів через електронну пошту та мережеві сервіси, а також формує журнали подій і звіти щодо інцидентів інформаційної безпеки.

Таким чином, у межах даного підрозділу було розроблено комплекс заходів захисту інформації для ТОВ «МАК-СЕРВІС», який включає контроль зовнішніх носіїв інформації, моніторинг електронної пошти, контроль конфіденційних документів, журналювання подій та систему сповіщення про інциденти. Реалізація зазначених заходів дозволить суттєво знизити ризик витоку конфіденційної інформації та підвищити загальний рівень інформаційної безпеки підприємства.

3.6. Оцінка ефективності запропонованих заходів

Для визначення ефективності запропонованої системи захисту інформації було проведено оцінювання рівня захищеності інформаційної інфраструктури ТОВ «МАК-СЕРВІС» до та після впровадження запропонованих заходів безпеки.

Під час аналізу інформаційної інфраструктури підприємства було встановлено відсутність централізованого контролю передачі інформації, моніторингу дій користувачів та засобів запобігання витоку конфіденційних даних. У результаті розробки системи захисту на основі SearchInform DLP було запропоновано комплекс заходів, спрямованих на усунення виявлених недоліків та підвищення рівня інформаційної безпеки підприємства [27; 38].

Для оцінки ефективності було виконано порівняння основних показників стану захисту інформації до та після впровадження запропонованих заходів (табл. 3.6).

Порівняння стану захищеності інформації до та після впровадження DLP-системи

Таблиця 3.6

Показник	До впровадження	Після впровадження
Контроль USB-пристроїв	Відсутній	Реалізовано
Контроль електронної пошти	Відсутній	Реалізовано
Моніторинг дій користувачів	Відсутній	Реалізовано
Контроль конфіденційних документів	Відсутній	Реалізовано
Журналювання подій	Відсутнє	Реалізовано
Сповіщення про інциденти	Відсутні	Реалізовано
Контроль мережевого трафіку	Відсутній	Реалізовано

Аналіз даних таблиці 3.6 свідчить про те, що впровадження SearchInform DLP дозволяє усунути основні недоліки системи захисту інформації підприємства. Найбільший ефект досягається за рахунок централізованого контролю каналів передачі інформації, моніторингу дій користувачів та своєчасного виявлення інцидентів інформаційної безпеки.

Для наочного відображення результатів оцінки ефективності запропонованих заходів побудовано діаграму рівня захищеності інформаційної системи до та після впровадження DLP-системи (рис.3.6).

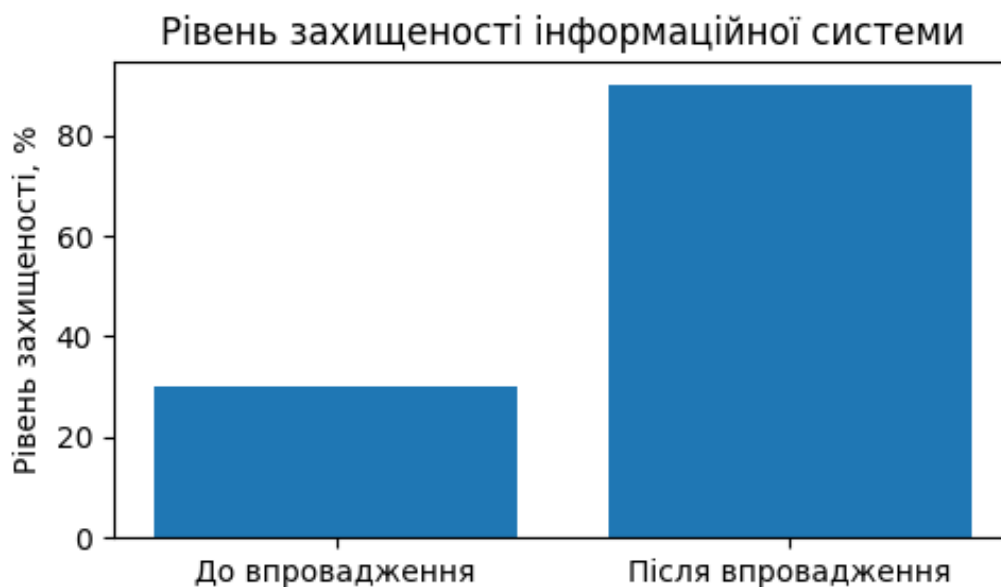


Рисунок 3.6 – Рівень захищеності інформаційної системи до та після впровадження DLP

Як показано на рисунку 3.6, після впровадження запропонованої системи захисту відбувається суттєве підвищення рівня контролю інформаційних потоків та зменшення ризику витоку конфіденційної інформації. Використання SearchInform DLP забезпечує постійний моніторинг дій користувачів, контроль використання зовнішніх носіїв, аналіз електронної пошти та централізоване журналювання подій безпеки.

Крім підвищення рівня захищеності інформації, запропоноване рішення дозволяє скоротити час реагування на інциденти інформаційної безпеки та спростити процес їх розслідування. Наявність журналів подій та автоматичних сповіщень забезпечує оперативне виявлення підозрілої активності та своєчасне реагування з боку адміністратора безпеки [32; 36].

Таким чином, результати проведеної оцінки свідчать про доцільність впровадження SearchInform DLP у ТОВ «МАК-СЕРВІС». Запропонована система захисту дозволяє усунути виявлені недоліки інформаційної безпеки, підвищити рівень контролю інформаційних потоків та забезпечити ефективний захист конфіденційної інформації від витоку.

3.7. Висновки до розділу 3

У третьому розділі дипломної роботи було розроблено систему захисту інформації ТОВ «МАК-СЕРВІС» від витоку конфіденційних даних на основі DLP-технологій. На основі результатів аналізу інформаційної інфраструктури підприємства побудовано модель внутрішнього порушника та визначено основні канали можливого витоку інформації, серед яких USB-носії, електронна пошта, локальна мережа та хмарні сервіси.

Для забезпечення контролю інформаційних потоків проведено аналіз сучасних DLP-рішень та обґрунтовано вибір системи SearchInform DLP як найбільш придатної для використання в умовах ТОВ «МАК-СЕРВІС». На основі обраного рішення розроблено архітектуру системи захисту інформації, що передбачає використання центрального сервера керування та агентів моніторингу на робочих станціях користувачів.

У межах реалізації заходів захисту розроблено політики контролю USB-пристроїв, електронної пошти, конфіденційних документів та журналювання подій інформаційної безпеки. Запропоновані заходи дозволяють здійснювати моніторинг дій користувачів, контролювати передачу службової інформації та своєчасно виявляти інциденти інформаційної безпеки.

Проведена оцінка ефективності показала, що впровадження SearchInform DLP дозволяє усунути виявлені недоліки системи захисту інформації підприємства, забезпечити контроль основних каналів витоку даних та підвищити загальний рівень інформаційної безпеки. Отримані результати підтверджують доцільність впровадження запропонованої системи захисту в інформаційній інфраструктурі ТОВ «МАК-СЕРВІС».

ВИСНОВКИ

У кваліфікаційній бакалаврській роботі виконано дослідження проблеми захисту інформації організації від витоку конфіденційних даних та розроблено систему захисту інформації на основі технології Data Loss Prevention для ТОВ «МАК-СЕРВІС». Актуальність обраної теми обумовлена зростанням кількості внутрішніх загроз інформаційній безпеці підприємств, які пов'язані з несанкціонованим доступом до інформації, її копіюванням, передачею через мережеві сервіси та використанням зовнішніх носіїв інформації.

У ході виконання роботи було розглянуто теоретичні основи забезпечення інформаційної безпеки підприємства та досліджено особливості захисту інформації від внутрішніх загроз. Проведено аналіз поняття внутрішнього порушника, розглянуто його основні типи та можливі способи реалізації загроз. Визначено, що витік конфіденційної інформації є однією з найбільш небезпечних загроз для діяльності сучасних підприємств, оскільки може призводити до фінансових втрат, порушення ділової репутації та втрати конкурентних переваг. Також було проаналізовано сучасні DLP-технології та встановлено, що їх використання дозволяє здійснювати контроль інформаційних потоків і своєчасно виявляти спроби несанкціонованої передачі даних.

У процесі дослідження інформаційної інфраструктури ТОВ «МАК-СЕРВІС» проведено аналіз локальної мережі підприємства, серверного обладнання, програмного забезпечення та системи контролю доступу. Визначено основні інформаційні активи підприємства, місця їх зберігання та категорії користувачів, які мають доступ до службової інформації. За результатами аналізу встановлено, що на підприємстві відсутні спеціалізовані засоби контролю передачі конфіденційної інформації через зовнішні носії, електронну пошту та мережеві сервіси. Також виявлено недостатній рівень централізованого моніторингу дій користувачів, що створює передумови для реалізації внутрішніх загроз та витоку службових даних.

На основі отриманих результатів було побудовано модель внутрішнього порушника та визначено основні канали можливого витоку інформації. Проведений аналіз показав, що найбільшу небезпеку для підприємства становлять USB-носії, електронна пошта, локальна мережа та хмарні сервіси. Для усунення виявлених недоліків виконано порівняльний аналіз сучасних DLP-рішень та обґрунтовано вибір системи SearchInform DLP як найбільш придатного засобу захисту інформації для умов ТОВ «МАК-СЕРВІС».

У практичній частині роботи розроблено систему захисту інформації на основі SearchInform DLP, яка включає архітектуру системи, механізми контролю зовнішніх носіїв інформації, електронної пошти, конфіденційних документів та централізованого журналювання подій інформаційної безпеки. Для реалізації заходів захисту сформовано політики безпеки, що визначають правила контролю інформаційних потоків та порядок реагування на виявлені інциденти. Запропоновані рішення дозволяють здійснювати постійний моніторинг дій користувачів, контролювати передачу службових документів та своєчасно виявляти порушення встановлених політик безпеки.

З метою оцінки результативності розроблених заходів проведено порівняння стану захищеності інформаційної системи підприємства до та після впровадження DLP-системи. Результати оцінювання свідчать про суттєве підвищення рівня контролю інформаційних потоків, появу можливості централізованого моніторингу дій користувачів, контролю передачі файлів через різні канали зв'язку та оперативного реагування на інциденти інформаційної безпеки. Впровадження запропонованої системи дозволяє значно знизити ризик витоку конфіденційної інформації та підвищити загальний рівень захисту інформаційних ресурсів підприємства.

Таким чином, мету дипломної роботи досягнуто, а поставлені завдання виконано в повному обсязі. Розроблена система захисту інформації на основі SearchInform DLP може бути рекомендована для впровадження в інформаційній інфраструктурі ТОВ «МАК-СЕРВІС» з метою забезпечення ефективного

контролю інформаційних потоків, протидії внутрішнім загрозам та підвищення рівня інформаційної безпеки підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – Київ : СофтПрес, 2005. – 316 с.
2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки / В.Л. Бурячок. – Київ : НАУ, 2013. – 432 с.
3. Василенко В.О. Інформаційна безпека підприємства / В.О. Василенко. – Київ : Центр навчальної літератури, 2008. – 136 с.
4. Гнатюк С.О. Основи кібербезпеки / С.О. Гнатюк. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 456 с.
5. ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. – Чин. від 1996-01-01. – Київ : Держстандарт України, 1995. – 38 с.
6. ДСТУ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання. – Київ : Держспоживстандарт України, 2007. – 47 с.
7. Закон України «Про захист інформації в інформаційно-комунікаційних системах». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
8. Закон України «Про інформацію». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12>
9. Закон України «Про основні засади забезпечення кібербезпеки України». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>
10. Закон України «Про захист персональних даних». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17>
11. Захист інформації в інформаційно-комунікаційних системах / Г.Ф. Конахович, О.Ю. Пузиренко. – Київ : Видавничий дім «Слово», 2005. – 288 с.
12. Корченко О.Г. Системи захисту інформації / О.Г. Корченко. – Київ : НАУ, 2004. – 264 с.

13. Корченко О.Г. Управління інформаційною безпекою / О.Г. Корченко. – Київ : Лазурит-Поліграф, 2010. – 412 с.
14. Кудін А.М. Кібербезпека та захист інформації / А.М. Кудін. – Київ : Ліра-К, 2021. – 380 с.
15. Ліпкан В.А. Інформаційна безпека України / В.А. Ліпкан. – Київ : КНТ, 2009. – 576 с.
16. Методи та засоби захисту інформації / В.О. Хорошко, О.А. Чекатков. – Київ : Юніор, 2003. – 504 с.
17. Нестеренко О.В. Основи технічного захисту інформації / О.В. Нестеренко. – Київ , 2006. – 240 с.
18. Петренко А.І. Безпека інформаційних систем / А.І. Петренко. – Київ: Академвидав, 2012. – 320 с.
19. Прохоров А.О. Захист інформації в комп'ютерних системах / А.О. Прохоров. – Харків : ХНУРЕ, 2011. – 356 с.
20. Руснак І.С. Інформаційна безпека та кібербезпека / І.С. Руснак. – Київ : НАОУ, 2015. – 304 с.
21. Сопілко І.М. Правові основи захисту інформації / І.М. Сопілко. – Київ : Освіта України, 2018. – 256 с.
22. Ткачук В.А. Захист інформації та кібербезпека / В.А. Ткачук. – Львів : Новий Світ-2000, 2019. – 312 с.
23. Bace R. Intrusion Detection / R. Bace. – Indianapolis : Macmillan Technical Publishing, 2000. – 320 p.
24. Bishop M. Computer Security: Art and Science / M. Bishop. – Boston : Addison-Wesley, 2018. – 1136 p.
25. Brown C. Computer Evidence Collection and Preservation / C. Brown. – Boston : Charles River Media, 2006. – 352 p.
26. Cybersecurity Framework 2.0. – National Institute of Standards and Technology, 2024. – Режим доступу: <https://www.nist.gov/cyberframework>
27. Forcepoint DLP. Data Loss Prevention Solutions. – Режим доступу: <https://www.forcepoint.com/product/dlp>

28. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva : International Organization for Standardization, 2022. – Режим доступу: <https://www.iso.org/standard/27001.html>
29. ISO/IEC 27002:2022 Information security controls. – Geneva : International Organization for Standardization, 2022. – Режим доступу: <https://www.iso.org/standard/75652.html>
30. McAfee Total Protection for DLP. – Режим доступу: <https://www.trellix.com/en-us/products/data-loss-prevention.html>
31. Microsoft Purview Data Loss Prevention. – Режим доступу: <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>
32. NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations. – Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
33. Northcutt S. Network Intrusion Detection / S. Northcutt. – Indianapolis : New Riders Publishing, 2002. – 512 p.
34. Peltier T. Information Security Policies, Procedures, and Standards / T. Peltier. – New York : Auerbach Publications, 2002. – 456 p.
35. Pfleeger C.P. Security in Computing / C.P. Pfleeger, S.L. Pfleeger. – New Jersey : Prentice Hall, 2015. – 800 p.
36. Scarfone K. Guide to Data Loss Prevention / K. Scarfone, M. Souppaya. – NIST, 2007. – Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-113/final>
37. Schneier B. Secrets and Lies: Digital Security in a Networked World / B. Schneier. – New York : Wiley Publishing, 2015. – 448 p.
38. SearchInform. DLP-система: принцип роботи та основні функції. – Режим доступу: <https://searchinform.ua/solutions/dlp/>
39. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards / W. Stallings. – Boston : Addison-Wesley, 2018. – 352 p.

40. Symantec Data Loss Prevention. – Broadcom Inc. – Режим доступа: <https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention>
41. Tipton H.F. Information Security Management Handbook / H.F. Tipton. – Boca Raton : CRC Press, 2013. – 1500 p.
42. Whitman M. Principles of Information Security / M. Whitman, H. Mattord. – Boston : Cengage Learning, 2021. – 656 p.
43. Wood C. Information Security Policies Made Easy / C. Wood. – San Francisco : Information Shield, 2007. – 720 p.
44. Zero Trust Architecture. – National Institute of Standards and Technology, 2020. – Режим доступа: <https://csrc.nist.gov/publications/detail/sp/800-207/final>
45. Zissis D. Addressing Cloud Computing Security Issues / D. Zissis, D. Lekkas // Future Generation Computer Systems. – 2012. – Vol. 28, No. 3. – P. 583–592.

Короткий звіт подібності

StrikePlagiarism.com

Звіт не був оцінений

Метадані

ДОКУМЕНТ

Заголовок
КБР_Веремейчук

Автор
Веремейчук

Науковий керівник / Експерт
Мирутенко Лариса Вікторівна,

ІД документу
334256527

ОРГАНІЗАЦІЯ

Назва організації
Kyiv National Economic University named after Vadym Hetman
KNEU

підрозділ
кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту
6/10/2026

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

0.95%

0.95%

КП 1

25

Довжина фрази для коефіцієнта подібності 2

0%

0%

КП 2

8289

Кількість слів

0.75%

0.75%

КЦ

69181

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		1

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Копіювати текст

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	http://lib.ru/lib/na:8080/hitstream/123456789/14610/1/%D0%9C%D0%BD%D1%81%D0%BB%D1%8	12 / 14 %\

F%D0%BA%20%D0%9E%D0%BB%D1%8C%D0%B3%D0%B0.pdf		
2	ВКР-Юрченко 11/12/2025 State University of Trade and Economics (State University of Trade and Economics)	12 (0.14 %)
3	Цвітко_EMM_ДР_перевірка 6/7/2025 Oles Honchar Dnipro National University (Факультет економіки)	11 (0.13 %)
4	БКР_КБ-409_Полесья_Д.О 2026 5/28/2026 National University "Lviv Politechnika" (NULP2)	10 (0.12 %)
5	КСЗІ КОХАН v3.0 11/20/2024 Kharkiv National University of Internal Affairs Course papers (Kharkiv National University of Internal Affairs Course papers)	10 (0.12 %)
6	Дипломна робота Єленовський І.В. 12/16/2025 Ukrainian national aviation university (ФКНТ Кафедра технічного захисту інформації)	7 (0.08 %)
7	Паламарчук Єльдар Безпека інформаційних систем н.кер. Яровий Р.О. 3/12/2026 European University (European University)	6 (0.07 %)
8	Паламарчук Єльдар Безпека інформаційних систем н.кер. Яровий Р.О. 3/12/2026 European University (European University)	6 (0.07 %)
9	Дипломна робота Єленовський І.В. 12/16/2025 Ukrainian national aviation university (ФКНТ Кафедра технічного захисту інформації)	5 (0.06 %)
База даних RefBooks 		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Домашня база даних 		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Програма обміну базами даних (0.81 %) 		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Паламарчук Єльдар Безпека інформаційних систем н.кер. Яровий Р.О. 3/12/2026 European University (European University)	12 (2) (0.14 %)
2	Дипломна робота Єленовський І.В. 12/16/2025 Ukrainian national aviation university (ФКНТ Кафедра технічного захисту інформації)	12 (2) (0.14 %)
3	ВКР-Юрченко 11/12/2025 State University of Trade and Economics (State University of Trade and Economics)	12 (1) (0.14 %)
4	Цвітко_EMM_ДР_перевірка 6/7/2025 Oles Honchar Dnipro National University (Факультет економіки)	11 (1) (0.13 %)

Список принятых фрагментов (фрагменты документов)		
5	БКР_КБ-409_Полесья_Д.О 2026 5/28/2026 National University "Lviv Politechnika" (NULP2)	10 (1) (0.12 %)
6	КСЗІ КОХАН v3.0 11/20/2024 Kharkiv National University of Internal Affairs Course papers (Kharkiv National University of Internal Affairs Course papers)	10 (1) (0.12 %)
Інтернет (0.14 %)		
#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
7	http://lib.pu.if.ua:8080/bitstream/123456789/14610/1/%D0%9C%D0%B0%D1%81%D0%BB%D1%8F%D0%BA%20%D0%9E%D0%BB%D1%8C%D0%B3%D0%B0.pdf	12 (1) (0.14 %)
 Список принятых фрагментів		
#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)