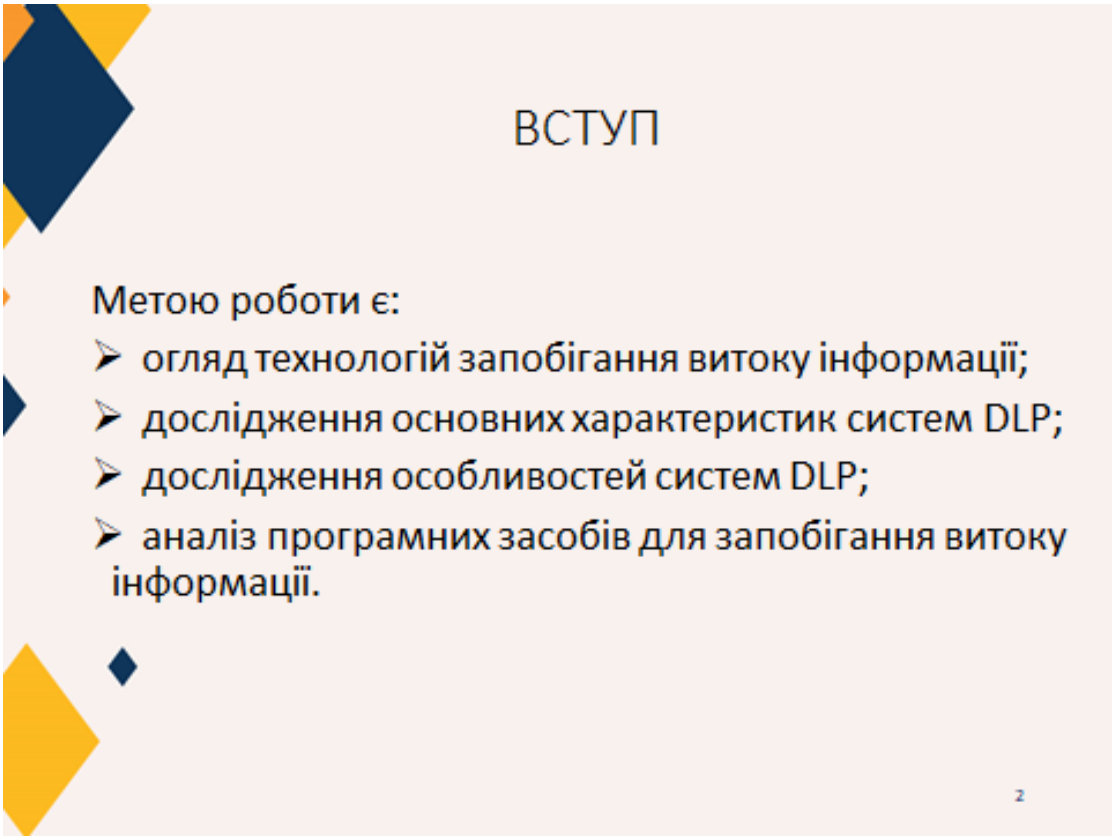
# ДОДАТОК А
# СЛАЙДИ ПРЕЗЕНТАЦІЇ

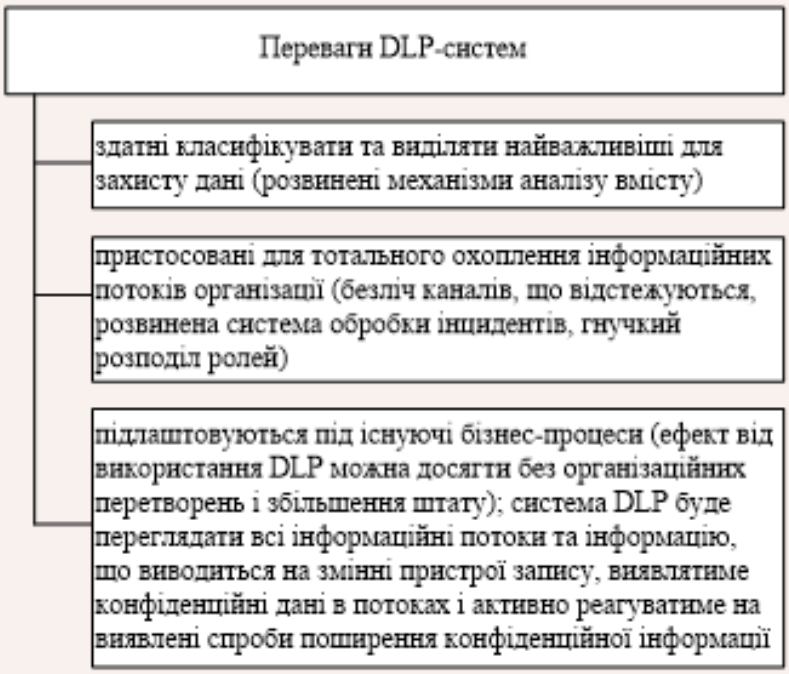

1 ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ
Основні причини для запобігання втрат даних
Зростання зовнішніх загроз і атак
Випадковий обмін інформацією
Внутрішні загрози
Поганий догляд BYOD
Хмарне сховище та послуги
Погана репутація в галузі
3


1 ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ
Технології захисту інформації
Антивірусне програмне забезпечення
Системи виявлення вторгнень (IDS)
Брандмауери
Системи запобігання вторгненням (IPS)
Системи запобігання витоку даних (DLP)
Управління інформацією та подіями безпеки (SIEM)
4

## 2 ОСНОВНІ ХАРАКТЕРИСТИКИ DLP-СИСТЕМ


5

## 2 ОСНОВНІ ХАРАКТЕРИСТИКИ DLP-СИСТЕМ




6

## 2 ОСНОВНІ ХАРАКТЕРИСТИКИ DLP-СИСТЕМ

**Недоліки DLP-систем**

- не містять вбудованих засобів шифрування
- методи класифікації даних, що використовуються в DLP та відповідні для глобального охоплення всіх оброблюваних ресурсів, можуть пропустити ті дані, якими система не була навчена

7

## 3 АНАЛІЗ СТАНІВ DLP-СИСТЕМИ

Метою DLP-систем є захист від витоку інформації протягом усього її життєвого циклу. На рис. 3.1 наведено три основні інформаційні стани:

- Data At Rest – інформація зберігається (знаходиться в стані спокою);
- Data In Motion – інформація передається в мережі;
- Data In Use – інформація використовується (обробляється).

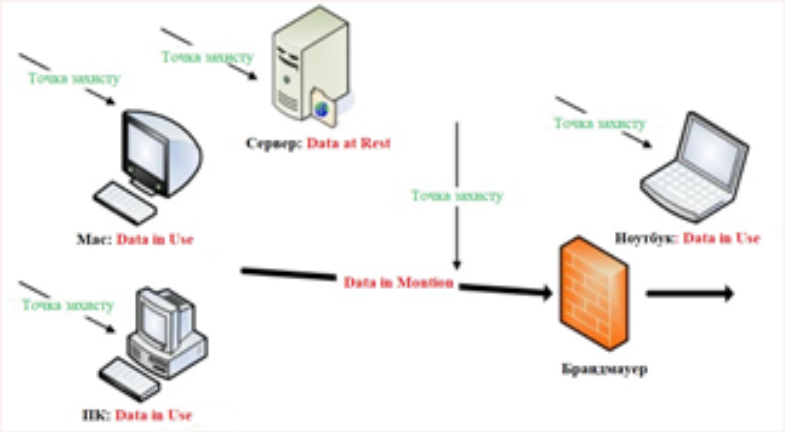



Рисунок 3.1 – Три основні інформаційні стани

8

## 4 ПРОГРАМНІ ЗАСОБИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

- Endpoint Protector by CoSoSys;
- Symantec DLP;
- McAfee DLP;
- Forcepoint DLP;
- SecureTrust Data Loss Prevention.

9

## 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Таблиця 5.1 – Порівняння програмного забезпечення DPL

| Програмне забезпечення DLP | Інструмент | Тип компаній | Платформи | Розгортання |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| **Endpoint Protector by CoSoSys** | Відкриття, відстеження та захист конфіденційних дані | Середні та корпоративні клієнти | Windows, Mac, Linux, принтери та тонкі клієнти | Віртуальний пристрій, хмарні послуги, розміщені в хмарі |
| **Symantec DLP** | Зменшення ризиків пору-шення даних і дотримання вимог | Підприємства | Windows, Mac, Linux | Хмарний і локальний |
| **McAfee DLP** | Захист від втрати даних | Малий і вели-кий бізнес | Windows, Mac, Linux | Хмарний і локальний |

10

# 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Продовження табл. 5.1

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Forcepoint DLP** | Дані контролюються за допомогою єдиної політики | Малий і великий бізнес, агентства та підприємства | Windows і веб-додаток | Хмарна основа |
| **SecureTrust Data Loss Prevention** | Знаходження, відстеження та захист даних у всіх станах: Data At Rest, Data In Motion та Data In Use | Бізнес усіх галузей | Windows, Mac, Linux | Хмарний і локальний |

11

# 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Таблиця 5.2 – Аналіз програмних засобів запобігання витоку інформації

| Фактор | Класифікатор | Коефіцієнт | Назва програмного засобу | | | | |
|---|---|---|---|---|---|---|---|
| | | | Endpoint Protector by CoSoSys | Symantec DLP | McAfee DLP | Forcepoint DLP | SecureTrust DLP |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Платформи** | Windows | 0,1 | + | + | + | + | + |
| | Mac | | + | + | + | | + |
| | Linux | | + | + | + | | + |
| | Принтер | | + | | | | |
| | Тонкий клієнт | | + | | | | |
| | Web-додатки | | | | | + | |
| **Результат** | | | 0,5 | 0,3 | 0,3 | 0,2 | 0,3 |

12

# 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Продовження табл. 5.2.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| **Розгортання** | Віртуальний пристрій | 0,15 | + | | | | |
| | Розміщення в хмарі | | + | | | | |
| | Хмарні послуги | | + | | | | |
| | Хмарна основа | | | | | + | |
| | Хмарний і локальний | | | + | + | | + |
| **Результат** | | | 0,45 | 0,15 | 0,15 | 0,15 | 0,15 |

13

# 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Продовження табл. 5.2.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| **Безкоштовний пробний період** | Так | 0,05 | + | | | + | |
| | Ні | | | + | + | | + |
| **Результат** | | | 0,05 | 0 | 0 | 0,05 | 0 |
| **Інтеграція** | Мережа | 0,1 | + | + | + | + | + |
| | Сховище | | + | + | + | + | + |
| | Хмара | | + | + | + | + | + |
| | Кінцева точка | | + | + | + | + | + |
| **Результат** | | | 0,4 | 0,4 | 0,4 | 0,4 | 0,4 |
| **Загальний результат** | | | 1,4 | 0,85 | 0,85 | 0,8 | 0,85 |

14

# 5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

За результатами аналізу було побудовано діаграму оцінок програмних засобів

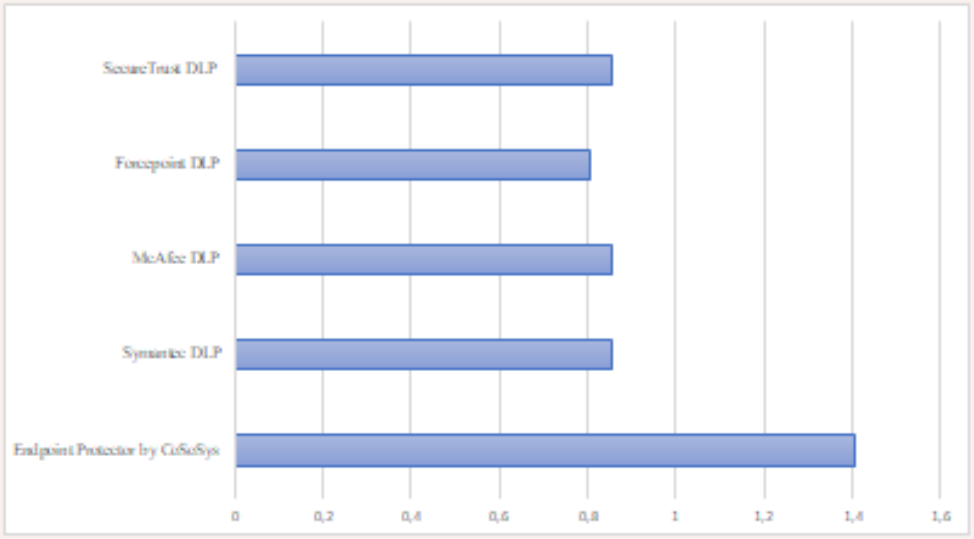



Рисунок 5.1 – Оцінка програмних засобів

15

# ВИСНОВКИ

В роботі підкреслено важливість захисту інформації, оскільки відбувається стрімке зростання інформації, і тому підприємствам стає важко відстежувати, захищати та керувати конфіденційними даними в межах корпоративних кордонів.

Рішення DLP допомагають підприємствам запобігати витоку інформації та реагувати на інциденти.

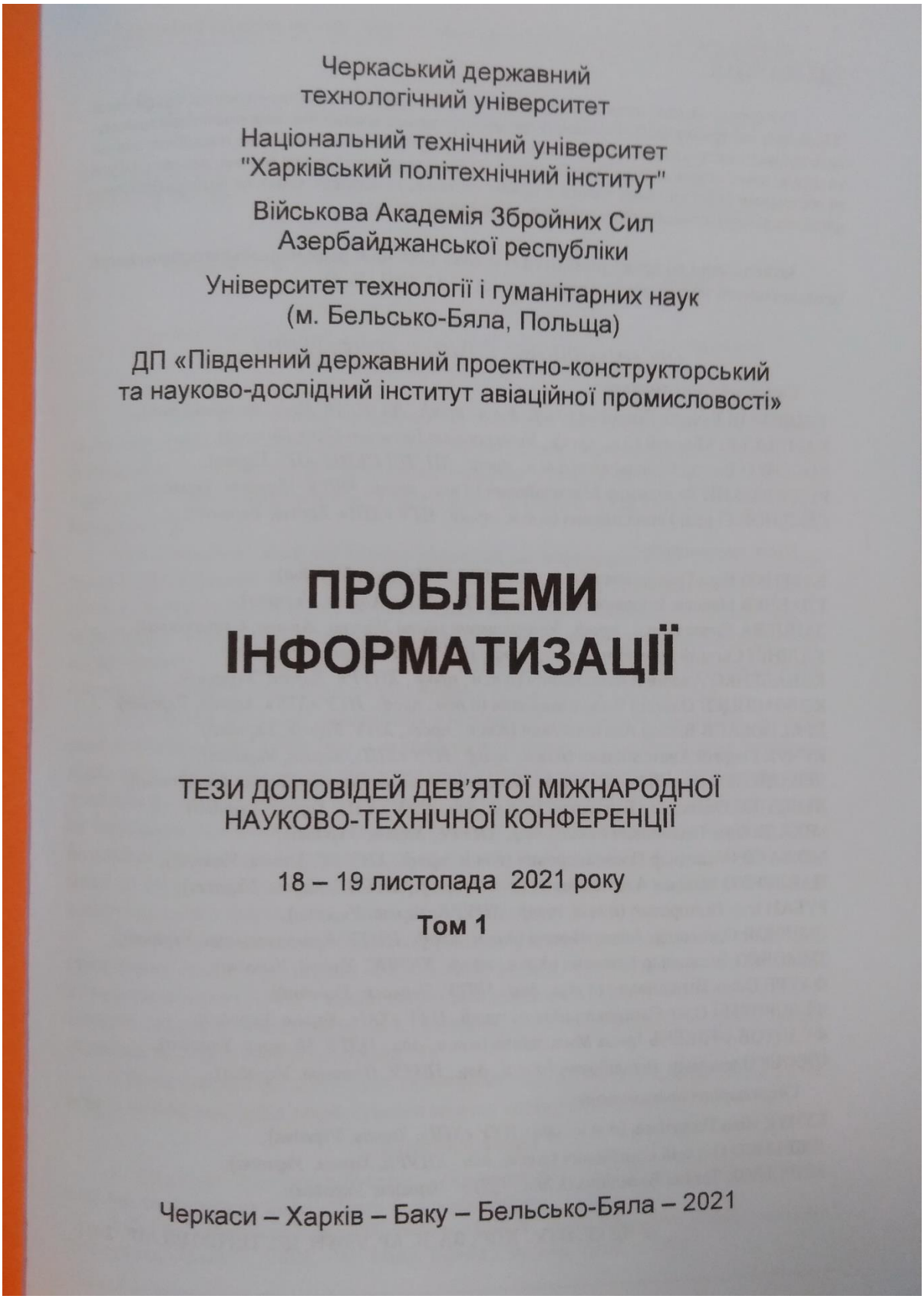
Було проаналізовано ефективність використання різних програмних засобів в залежності від типу організації.

За результатами оцінки програмних засобів для запобігання витоку інформації було встановлено, що найбільш ефективним є програмний продукт Endpoint Protector by CoSoSys.

16


Дякую за увагу!
17

ДОДАТОК Б
ПУБЛІКАЦІЯ ЗА ТЕМАТИКОЮ РОБОТИ



Черкаський державний
технологічний університет

Національний технічний університет
"Харківський політехнічний інститут"

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

# ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

ТЕЗИ ДОПОВІДЕЙ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

18 – 19 листопада 2021 року

**Том 1**

Черкаси – Харків – Баку – Бельсько-Бяла – 2021

Секція 3

# АНАЛІЗ ТЕХНОЛОГІЙ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Чеботарьова Д.В., Пестєрєва С.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

У зв'язку зі стрімким розвитком технологій інформація є більш доступною, зростають обсяги даних, що зберігаються та передаються в мережах, крім того переважна більшість даних є конфіденційними [1]. Підтримка безпеки даних дуже важлива, оскільки навіть невелика втрата даних може створити критичний вплив на організацію. Саме тому запобігання витоку конфіденційних даних є важливою актуальною задачею.

Традиційно організація впроваджувала такі методи, як формування політики в організації, впровадження брандмауера, віртуальної приватної мережі на кінцевих точках, але ці методи почали відставати, оскільки технології витоку і крадіжки даних постійно розвиваються. Тому виникла потреба в системі, яка могла б запобігти витоку даних.

Найкращим рішенням для запобігання ненавмисних витоків даних є впровадження автоматизованої корпоративної політики, яка виявляє захищені дані до того, як вони залишать організацію. До таких рішень відносять технології запобігання витоку конфіденційної інформації з інформаційних систем та мереж Data Loss Prevention (DLP).

**Метою доповіді** є аналіз компонентів і методів запобігання витоку інформації, а також розробка рекомендацій щодо використання цих методів при захисті інформації в інформаційних системах та мережах.

Методи DLP ідентифікують, відстежують та захищають передачу даних шляхом глибокої перевірки вмісту та аналізу параметрів транзакції (таких як джерело, призначення, об'єкт даних і протокол) із централізованою структурою керування [2]. Методи DLP виявляють та запобігають несанкціоновану передачу конфіденційної інформації.

В роботі описано важливість збереження конфеденційності інформації для організацій та можливі наслідки витоку корпоративних даних. Було проаналізовано та досліджено існуючі системи, що використовуються для захисту даних, та технології DLP з точки зору їх компонентів і методів, що використовуються в них, а також відмінності між ними.

## Список літератури

1. Sheela Gowr. P, Kumar. N. Data Leakage Prevention System: A Systematic. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. DOI: https://www.ijrte.org/wp-content/uploads/papers/v8i4/D6904118419.pdf.

2. Data Loss Prevention R76 Administration Guide. Introduction to Data Loss Prevention. *Check Point Software Technologies Ltd.* 2014. DOI: https://sc1.checkpoint.com/documents/R76/CP_R76_DLP_WebAdmin/62453.htm.

| Позначення | Найменування | Дод. відомості |
|---|---|---|
| | Текстові документи | |
| 1. | Пояснювальна записка | 66 с. |
| | Графічні документи | |
| | Слайди презентації | 17с. |

| Змін. | Арк. | Номер докум. | Підпис | Дата | | | | |
|---|---|---|---|---|---|---|---|---|
| Розроб. | | Пестєрєва | | | Аналіз програмних засобів запобігання витоку інформації | Літ. | Аркуш | Аркушів |
| Перевір. | | Чеботарьова | | | | У | 1 | 1 |
| | | | | | | ХНУРЕ кафедра ІМІ | | |
| Н. контр. | | Чеботарьова | | | | | | |
| Затв. | | Безрук | | | Відомість атестаційної роботи | | | |