МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Західноукраїнський національний університет

Факультет комп’ютерних інформаційних технологій

Кафедра кібербезпеки

ХАРЧУК Олександр Віталійович

Інформаційна безпека телекомунікаційних систем на основі DLP технології / Information security of telecommunication systems based on DLP technology

спеціальність 125 Кібербезпека

освітньо-професійна програма - Кібербезпека

кваліфікаційна робота

Виконав студент групи КБм-21

О.В. Харчук

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Науковий керівник:

д.т.н., професор В.В. Яцків

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Яцків

підпис

Тернопіль – 2021

РЕЗЮМЕ

**Тема роботи** розкрита у кваліфікаційній роботі обсягом 94 сторінок та містить 3 розділи. Складається з 11 ілюстрацій, 11 таблиць, 41 літературних посилань.

**Основна мета роботи** полягає у підвищенні рівня захищеності шляхом використання DLP-систем. Для цього треба провести дослідження існуючих на ринку систем DLP, розкрити їх слабкі сторони і знайти шляхи покращення їх роботи.

**Об'єктом дослідження** виступають такі системи DLP, як Sуmаntес, SеаrсhІnfоrm, Zесurіоn Zgаtе, Sесurе Tоwеr та інші.

Як **предмет дослідження** розглядається здатність систем DLP реагувати на інциденти, пов'язані з витоком інформації.

При написанні роботи було проведено ознайомлення з літературою, тестування і аналіз DLP-систем, було знайдено гіпотетичні рішення існуючих проблем та розроблено доповнення, яке можна інтегрувати з DLP-системами для покращення їх функціонування.

**Наукова новизна роботи** полягає у розробленні відомостей щодо ефективності використання DLP систем.

**Результатом** є гіпотетичне рішення для усунення недоліків та підвищення ефективності систем DLP, а також розробка доповнення, яке можна інтегрувати з іншими рішеннями DLP.

АBSTRАСT

**The topic of the research** is revealed in the qualification work of 94 pages and consists of 3 sections. Contents 11 illustrations, 11 tables, 41 links.

**The main purpose** of this work is to increase the level of security with DLP-systems. Is nесессаrу tо сонудt ресеарсh оn ехистинг DLP sустems на thе mаrkеt, tо rеvеаl thеіr wеаknеssеs аnd fіnd wауs pе tо іmprо іmprе.

**The object of research** is such DLP systems as Sumantes, SearshInform, Zesurion Zgate, Sesure Tower and others.

**The subject of the study** is the ability of DLP systems to respond to incidents related to content-related information.

During writing qualifisation thy work, thy literatury was reviewed, tested BV analuzed DLP-off sustems, theaya weaya hupothetisal found solutions to problems ehisting BV additions were developed that used to service with integrated DLP-sustems to improve their funstionaliy.

**Scientific knowledge** of the work is the development of information on the effectiveness of DLP systems.

**The result** is a hypothetical solution to solve short problems and efficiency of DLP systems, as well as the development of the add-tgr.

ВСТУП

**Актуальність теми.** Рівень інформаційної безпеки є важливим критерієм ефективності функціонування для кожного підприємства, зокрема і у сфері ІT. Забезпечення потрібного рівня інформаційної безпеки досягається за допомогою застосування різноманітних засобів та заходів, за допомогою створення комплексної системи захисту інформації.

Проблема витоку інформації є дуже актуальною. Значний відсоток витоку відбувається шляхом порушення політики безпеки, несанкціонованого доступу, навмисного та випадкового. Високий рівень безпеки інформації бізнесу здійснюється через розробку ефективної політики безпеки і, в результаті, оптимальних правил розмежування надання доступу. Методи, що реалізують політику безпеки, здійснюють контроль над взаємодією інформаційних ресурсів та користувачів, є основною частиною підсистеми управління доступу. Збільшення ефективності роботи цих методів є важливим завданням.

Поширеність методів захисту інформації (Gаrtnеr говорить, що близько третя частина компаній вже користуються DLP) знімає тільки частину проблеми-випадкові витоки, – не впливають на зловмисні жодним чином. Питання тут скоріше в сприйнятті DLP-систем як ПЗ, здатного самостійно, без жодних сумнівів з боку служб безпеки даних, боротися з витоками, що є зовсім неправильно. І якщо з випадковими витоками DLP справді справляється, то боротьба із шкідливими програмами потребує серйозної консалтингової частини в DLP проєктах на етапі планування введення та супроводу системи, розслідувань випадків.

Розпізнавання секретної інформації в DLP-системах розробляється декількома методами: аналізом формальних властивостей (наприклад, гриф документа, міток введених з наміром, порівнянням хеш-функції) і аналізом наповнення системи.

Перший метод дозволяє уникнути неправильних спрацьовувань (помилок першого порядку), але зате потребує попередньої класифікації документів, застосування міток, збору сигнатур і так далі. Пропуски секретних даних (помилки другого роду) при цьому методі цілком вірогідні, якщо конфіденційний документ не піддався попередньої класифікації. Другий спосіб дає помилкові спрацьовування, зате дозволяє виявити пересилання секретної інформації не тільки серед документів з грифом. У хороших DLP-системах обидва способи поєднуються.

Через цей тренд застосування способів та моделей управління інформаційною безпекою в ІТС підприємства із застосуванням DLP-систем є актуальним та відкритим питанням.

# 1 АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

* 1. Аналіз стану та забезпечення безпеки інформаційної безпеки на підприємствах

За 2019 рік у світі було зафіксовано понад 1200 випадки витоку секретної інформації, яка на 19% перевищує дані минулих досліджень.

Офіційно заявлені в ЗМІ ушкодження кредитно-фінансових установ від витоків у першому півріччі 2020 року досягли трішки більше ніж 45,6 млн. доларів США.

Сфальсифіковано більш ніж 1,3 млрд записів, у тому числі грошова та персональна інформація.

Частина випадкових витоків постійно зменшується і досягає 39%.

Збільшується частина витоків у державних компаніях і муніципальних організаціях – 27% (+ 9% порівняно з 2018 роком).

Лідируючий тип витоків – персональні дані – 89,2%.

Найпопулярніший канал витоків – паперова документація 21,6% [23].

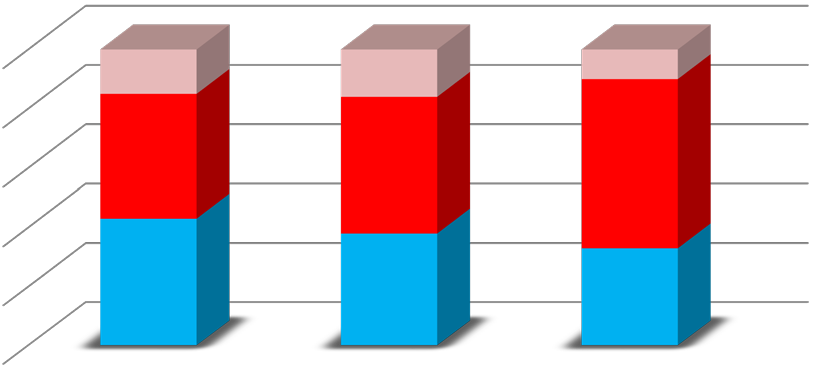
У 2019 році Аналітичний центр InfoWatch зареєстрував велику кількість прикладів витоку інформації з компаній корпоративного та державного секторів.

Персональні дані понад 31 мільйона користувачів Smart Keyboard Tours AI tupé для пристроїв Android просочилися в Інтернет. Розробники не обмежували доступ до сервера, на якому встановлена база даних. Про це повідомляє портал ZDNet.

Сервер належить засновнику програми AITupe Ейтану Фітусі. Ресурс не був захищений паролем, що теоретично може дозволити будь-якому користувачеві Інтернету отримати доступ до великої бази даних розміром близько 577 ГБ. Цю помилку виявили дослідники безпеки з Kromtech.

Крім того, фахівці Kromtech знайшли кілька великих таблиць з дуже «м’якими» даними з пристроїв користувача. Один показує 10,7 мільйона адрес електронної пошти, інший 374,6 мільйона телефонних номерів. Серед інших файлів були дані про завантажені програми, зокрема банківські [13]

Аналітики InfoWatch відзначають, що впровадження захисту вплине на співвідношення випадкових і навмисних витоків. Інструменти та методи, доступні на ринку, ефективніші проти випадкових витоків, ніж навмисні. Як бачимо, відсоток випадкових витоків дійсно знижується – у 2018 році частка випадкових витоків становила 43%. На цьому тлі зростає частка шкідливих джерел – 42%. (Відсото витоків невідомого характеру не змінився – 16% у 2019 році).



0

20

40

60

80

100

**2018**

**2019**

**2020**

**43**

**38**

**33**

**42**

**46**

**57**

**15**

**16**

**10**

**Розподіл навмисних і ненавмисних витоків**

**інформації**



**Випадкові**



**Навмисні**



**Не визначено**

Рисунок 1.1 – Розподіл навмисних і ненавмисних витоків, 2018-2020 рр.

Як згадувалося раніше, найяскравіше зазначена тенденція проявляється в «передових» з точки зору ІБ галузях – банки, телекомунікаційні підприємства. Там частка випадкових витоків по відношенню до зловмисних ще менше.

**42**

**22**

**19**

**9**

**8**

**2018**

**Комерційні**

**Державні**

**Освітні**

**Медичні**

**Не встановлено**

Рисунок 1.2 – Розподіл витоку інформації за підприємствами

Аналізуючи статистичні показники розподілу витоків за 2018-2020 років, можна відмітити зниження рівня витоків в освітніх організаціях до 12%, в порівнянні з 19% в 2018 році. Збільшення частки витоків комерційних та державних організаційпояснюється направленими діями у зв’язку веденням інформаційної війні між державами.

Захист даних є однією з головних проблем при впровадженні хмарних сервісів. Середньостатистичне підприємство використовує 1427 хмарних сервісів, і співробітники часто вводять нові сервіси самостійно. Аналізуючи дані про використання хмари для 30 мільйонів користувачів, McAfee (раніше Skyhigh Networks) виявила, що 18,1% документів, завантажених до файлообмінних служб, містять конфіденційну інформацію, таку як особиста інформація (PII), захищена інформація про здоров’я (PHI), дані платіжних карт або інтелектуальна власність, що створює проблеми з дотриманням вимог. Звідси випливає, що використання правильного рішення DLP у хмарі, що включає точність, моніторинг у режимі реального часу, аналіз даних у русі, усунення інцидентів та розробку політики втрати даних, є важливим для успішного впровадження хмари.

### 1.1.1 Статистика розподілу витоків за каналами

Канал витоку - це характеристика, що має безпосереднє практичне застосування. Залежно від частоти та ймовірності витоків у конкретному каналі можна спланувати реалізацію захисту, а також визначити пріоритетність – на які канали слід звертатися в першу чергу. Але крім статистики, необхідно враховувати інформаційні потоки та методи передачі інформації та специфіку бізнес-процесів.

На рисунку 1.3 показано розподіл витоків у каналах.

За результатами розподілу поширених каналів витоку, на першому місці йдуть канали паперу, ПК, ноутбуків і смартфонів. Витік інформації через папір залишається актуальним і суттєвим.

Однією з проблем із запобіганням витоку інформації з паперових документів є неможливість ефективно відстежувати паперові носії.

**20**

**,**

**1**

**,**

**17**

**4**

**9**

**,**

**10**

**6**

**8**

**,**

**1**

**20**

**,**

**1**

**2**

**9**

**,**

**2**

**,**

**8**

**2018**

**ПК**

**Ноутбуки, Сматрфони**

**Веб**

**Змінні носії**

**Електронна пошта**

**Паперові документи**

**Носії резервних копій**

**Інші**

а)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **9**  **,**  **4**  **19**  **,**  **2**  **9**  **,**  **4** | **2019**  **21**  **,**  **9**  **18**  **11**  **,**  **5**  **5**  **,**  **3**  **5**  **,**  **3** | **9**  **,**  **8**  **17**  **,**  **9** | **9**  **,**  **5**  **4**  **,**  **9** | **2020**  **3,1**  **12** | **23**  **19**  **,**  **8** |

*б) в)*

Рисунок 1.3 – Канали витоків інформації, 2018-2020 рр.

Витоки з ПК становлять значну частку і збільшуються. Основними причинами витоків з ПК є поширення доступу до ПК серед співробітників, використання неліцензійного програмного забезпечення.

Згідно зі звітом Ради директорів: глобальна інформація Ernst & Young за 2019 рік. За даними Survue, однієї з найбільших і найавторитетніших аудиторських компаній у світі Ernst & Young, 60% опитаних компаній повідомили про збільшення ризику через використання соціальних мереж, хмарних обчислень і портативних пристроїв. 64% респондентів назвали поширення важливих даних одним із 5 найбільших ризиків, а 74% увійшли до 5 найбільших ризиків безперервного доступу до критичних ІТ-ресурсів. У зв’язку з цим 50% опитаних компаній зазначили, що мають намір підвищити вартість впровадження систем запобігання витоку інформації. Одним з ефективних заходів для запобігання витоку даних є використання рішень DLP [7].

### 1.1.2 Забезпечення безпеки інформації циркулюючої на підприємствах

Три основні типи програмного забезпечення для запобігання втраті даних включають мережевий DLP, DLP кінцевої точки та Cloud DLP.

Мережевий DLP. Мережні рішення DLP забезпечують кращу видимість у мережі вашої компанії, дозволяючи таким чином контролювати потік інформації через мережу компанії, електронну пошту або інтернет. Програмне забезпечення DLP допомагає аналізувати мережевий трафік і встановлювати політику безпеки, щоб пом’якшити ризики втрати даних, забезпечуючи при цьому дотримання правил. Застосовуючи політику безпеки, програмне забезпечення DLP може виконувати певні заздалегідь встановлені дії, наприклад дозволяти, блокувати, позначати, аудит, шифрувати або поміщати на карантин підозрілі дії, які порушують політику інформаційної безпеки вашої компанії.

DLP кінцевої точки. Пристрої кінцевої точки, такі як настільні комп’ютери та ноутбуки, є основними інструментами сучасного бізнесу. Нове дослідження vArmour показало, що 76% співробітників США мають неналежний доступ до конфіденційних даних. Рішення Endpoint DLP відстежують кінцеві пристрої, такі як сервери, комп’ютери, ноутбуки та мобільні пристрої, на яких використовується, переміщується та зберігається важлива інформація вашої компанії. Це допомагає запобігти втраті ваших конфіденційних даних або неправомірному використанню неавторизованими особами.

Хмарний DLP. Оскільки компанії все частіше переміщують свої бізнес-дані та програми в хмарне середовище, хмарне DLP є життєво важливим для того, щоб запобігти витоку, втраті чи неправильній обробці критично важливих для бізнесу робочих навантажень. Хмарні рішення DLP захищають ваші дані, шифруючи конфіденційні дані та гарантуючи, що дані надсилаються лише в ті хмарні програми, які авторизовані вашою компанією. Сучасні передові хмарні технології DLP здатні ідентифікувати, класифікувати, видаляти або модифікувати конфіденційні дані, перш ніж вони будуть передані в хмарне середовище, щоб захистити ваші дані від кіберзагроз, зловмисних інсайдерів та випадкового розкриття.

Найкращі методи запобігання втраті даних. Визначте свою мету: чітко визначте, чого ви намагаєтеся досягти за допомогою програми запобігання втраті даних, чи це захист інтелектуальної власності, краща видимість і контроль над вашими даними чи виконання нормативних вимог. Наявність чіткої мети допоможе вам визначити, який тип рішень DLP включити у вашу стратегію запобігання втраті даних — мережевий, кінцевий або хмарний DLP.

Ідентифікація та класифікація даних: усі дані не однакові. Щоб краще захистити свої дані, ви повинні спочатку визначити дані, які є критичними для вашого бізнесу, як-от інформація про клієнта, фінансові записи, вихідні коди, креслення тощо, і класифікувати їх на основі їх рівня критичності.

Визначте політику безпеки даних: розробіть комплексні правила та політики безпеки даних і встановіть їх у мережі вашої компанії. Технології DLP можуть виконувати дії на основі заздалегідь запрограмованих правил для відстеження, аналізу та блокування доступу до конфіденційних файлів через незахищені джерела.

Керування доступом: обмежте доступ до конфіденційних даних. Доступ до критичної інформації та її використання має бути обмежено залежно від ролей та відповідальності користувачів. За допомогою інструментів DLP ваші системні адміністратори можуть призначати відповідні рівні авторизації користувачам залежно від типу даних, які вони обробляють, та їхніх рівнів доступу.

Навчайтеся та навчайте своїх співробітників: запобігання втраті даних є безперервним процесом, і ваші співробітники є важливою частиною програми. Тому навчання ваших співробітників важливості безпеки даних і наслідків втрати даних для вашого бізнесу відіграватиме важливу роль в успіху вашої програми DLP, адже люди вважаються найслабшою ланкою кібербезпеки.

Управління сучасною компанією є складним завданням, що вимагає організації взаємодії ресурсів різного типу.

До таких ресурсів належать, зокрема, інформаційні системи, що автоматизують бізнес-процеси компанії. Як правило, ІТ-інфраструктура компанії включає системи управління проектами, комунікаційні системи, бази даних, комп’ютерні мережі із серверами обробки та зберігання даних тощо.

Загрози інформаційної безпеки є складними: зовнішні зловмисники атакують мережі організацій та інформаційні ресурси, а їхні власні співробітники, навмисно чи ненавмисно, часто стають джерелами секретної інформації для третіх сторін. Зовнішні організації (конкуренти, преса, керівники) і, на жаль, ваші співробітники, які мають законний доступ до обробленої інформації, зацікавлені в отриманні доступу до багатьох категорій обробленої інформації, в тому числі до інформації про клієнтів та історії роботи з ними, персональні дані персоналу, документи стратегічного розвитку, внутрішні аналітичні звіти та багато іншого. [5]

Використання традиційних заходів безпеки, таких як антивірус і брандмауер, захищає інформаційні активи від зовнішніх загроз, але жодним чином не захищає інформаційні активи від витоку, спотворення або знищення інсайдерським зловмисником.

За статистикою, частка випадкових витоків у комерційних компаніях зменшується. Однією з причин цього явища є впровадження DLP-систем. З іншого боку, частка навмисних витоків все ще має тенденцію до збільшення. Це говорить про те, що системи DLP є більш ефективними для запобігання випадковим витокам, і, у випадку навмисних розпорядників, порушники достатньо кваліфіковані, щоб викрасти конфіденційну інформацію. [11]

Тому перед нами постає питання ефективності DLP-систем як засобу інтелектуальної власності бізнесу. Навмисні витоки представляють більшу потенційну загрозу, оскільки зловмисник має чітку мету і планує використати вкрадену інформацію.

Відповідно до статті 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» сукупністю інформаційно-телекомунікаційних систем, що виступають як єдине ціле в процесі обробки інформації, є інформаційно-телекомунікаційна система.

Банк і бази даних є сховищем інформації та основною складовою інформаційної системи в інтегрованій багаторівневій автоматизованій системі управління ІТ.

Основні вимоги до БД:

* інтеграція БД та цілісність кожної з них;
* незалежність;
* мінімальна втрата збережених даних;
* здатність до розширення [16].

1.2 Аналіз технологій DLP

Нижче наведено кілька кроків, які підприємства можуть зробити для впровадження програми DLP:

Проведіть інвентаризацію та оцінку. Підприємства не можуть захистити те, про що вони не знають. Повний інвентар є обов’язковим. Деякі продукти DLP — від таких постачальників, як Barracuda Networks, Cisco та McAfee — виконають повне сканування мережі.

Класифікувати дані. Організаціям потрібна система класифікації даних як для структурованих, так і для неструктурованих даних. Такі категорії включають персональну інформацію, фінансові дані, нормативні дані та інтелектуальну власність.

Встановити політику обробки даних і виправлення. Наступним кроком після класифікації даних є створення політик для їх обробки. Це особливо актуально для регульованих даних або для регіонів із суворими правилами, як-от у Європі з GDPR та Каліфорнії з CCPA.

Запровадити єдину централізовану програму DLP. Занадто багато організацій впроваджують кілька DLP в різних відділах і бізнес-підрозділах. Це призводить до неузгодженості захисту і відсутності повної картини мережі. Повинна бути одна комплексна програма.

DLP-системи засновані на аналізі потоків даних, які перетинають периметр захисту інформаційної системи. При виявленні секретної інформації в цьому потоці спрацьовує активний компонент системи, і передача повідомлення (пакет, потік, сеанс) блокується.

Як окремий програмний продукт DLP система характеризується наявністю наступної функціональності:

* DLP системи аналізують вихідний трафік;
* DLP-системи аналізують інформаційні потоки за допомогою кількох технологій.

Сьогодні DLP-системи є потужною розподіленою інформаційною системою з єдиним центром управління, а також низкою елементів, що забезпечують безпосередню реалізацію прикладних функцій захисту інформації на керованих елементах інформаційної інфраструктури.Залежно від архітектури побудови і умов функціонування сучасні DLP-системи можна поділити на наступні класи, які наведені в таблиці 1.1.

Система DLP зазвичай складається з багатьох компонентів. Типове рішення DLP зазвичай включає:

Центральний сервер управління, який виконує такі функції:

* об'єднання компонентів рішення в єдину систему;
* ідентифікація даних, що містять секретну інформацію;
* створення, редагування та поширення політики роботи з конфіденційними даними;
* збір, зберігання та обробка інцидентів, створення та розповсюдження звітів;
* забезпечення рольового доступу до управління системою співробітникам інформаційної безпеки.

Таблиця 1.1 – Архітектура DLP-систем

|  |  |
| --- | --- |
| Назва класу | Опис класу |
| Периметрові | Системи, які встановлюються на розриві каналу або отримують дзеркальне відображення трафіку.  До цього класу також належать системи, які інтегровані в компоненти інфраструктури (поштові сервери, веб-сервери, сервери друку тощо) на рівні відповідних до них плагінів і забезпечують функціональність захисту від витоків на рівні мережі. |
| Агентські | Системи, агенційні модулі яких встановлені на робочих станціях і несуть основні функції захисту від витоків на рівні робочої станції. |
| Гібридні | Найбільш універсальні системи, до складу яких входять як периметральні, так і агентські елементи. |

Модулі для моніторингу та блокування секретної інформації, що передається по мережевих каналах. Їх можна представити як єдиний пристрій, що реалізує як функції, так і окремо (наприклад, Network Monitor, Network Prevention для Web, Network Prevention для електронної пошти).

Мережевий модуль аналізує загальний обсяг вихідного трафіку від компанії. Мережевий модуль не тільки перевіряє витоки секретної інформації, а й може блокувати такі дії.Агенти для робочих станцій і серверів, що забезпечують контроль:

* переміщення секретної інформації на знімних носіях (USB, CD/DVD тощо);
* перенесення інформації в буфер обміну (функція «Вставити/Копіювати»);
* можливість зробити знімок з екрану («Print Screen»);

Також агенти виконують функцію пошуку секретної інформації на локальних дисках.

Агент на робочому місці контролює дії, які виконує співробітник з конфіденційними даними. Кожен агент рішення DLP оснащений власною функціональністю, але є базовий набір функцій, загальних для всіх рішень:

* блокування запису або аудит для USB-пристроїв;
* блокування або аудит запису CD/DVD;
* блокування або перевірка передачі конфіденційних документів на файлові сервери;
* блокування або аудит під час друку матеріалу на локальному або мережевому принтері.

Основні функції системи DLP:

Перша – це ідентифікація, тобто виявлення конфіденційних даних та їх зберігання в мережі компанії. Крім того, система може проаналізувати правомірність зберігання виявленої інформації в її поточному місці і, при необхідності, здійснити передачу в захищені репозиторії.

Друга функція – моніторинг, при якому система контролює передані дані та виявляє порушення відповідно до умов, встановлених у політиках.

Третя функція – захист. Ця функція може бути представлена різними діями. Це може включати надсилання сповіщень про політику безпеки, ізоляцію карантину та блокування передачі даних.

Захист секретної інформації здійснюється системою DLP за допомогою таких основних функцій:

* Фільтрація трафіку по всіх каналах передачі даних;
* Глибокий аналіз трафіку на рівні змісту та контексту.
* Захист секретної інформації в системі DLP відбувається на трьох рівнях: Data-in-Motion, Data-at-Rest, Data-in-Use.

Data-in-Motion - дані, що передаються по мережевих каналах:

* Web (протоколи HTTP / HTTPS);
* Інтернет-месенджери (ICQ, QIP, Skype, MSN, WatsUpp, Telegram і так далі);
* Корпоративна та особиста пошта (POP, SMTP, IMAP тощо);
* Бездротові системи (WiFi, Bluetooth, 3G тощо);
* FTP-з'єднання.

Data-at-Rest – дані, які статично зберігаються на:

* Сервери;
* Робочі станції;
* Ноутбуки;
* Системи зберігання (СТС).

На другому етапі, після впровадження організаційних методів, запровадження технічних засобів, що контролюють доступ до інформації та контролюють локальну мережу підприємства, запобігаючи витоку. [4]

При виборі конкретного рішення необхідно, щоб воно відповідало підходу компанії до захисту інформації. Умовно всі системи DLP можна розділити на активні, пасивні та комбіновані.

Пасивні системи DLP – це розслідування інцидентів, що сталися. Ці системи не можуть блокувати витік інформації, але можуть надати повну інформацію про джерело та канали витоку.

Цей тип систем почав розвиватися у відповідь на необхідність першого підходу до інформаційної безпеки, в якому пошук порушників є важливішим, ніж запобігання витоку секретної інформації. Ці системи складаються з трекерів-перехоплювачів, які копіюють усі електронні листи, що надсилаються через основні канали зв’язку: корпоративну та веб-пошту, соціальні мережі, обмін миттєвими повідомленнями, FTP, принтери та USB-носія.

Системи DLP зазвичай використовують три методи ідентифікації: імовірнісний, детермінований та комбінований. Системи, засновані на першому методі, переважно використовують аналіз мовного змісту та «відбиток пальця» даних. Ці системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацьовувань. Системи, які використовують детермінований підхід (мітки файлів), дуже надійні, але не мають гнучкості. Комбінований підхід поєднує обидва методи з аудитом середовища зберігання та обробки, що дозволяє досягти оптимального вирішення проблеми захисту конфіденційності інформації.

Усі корпоративні потоки даних проходять через систему DLP, і система повинна визначити, чи належать вони до того, що передається тому, хто захищається. Для цього використовують такі технології:

* + Підписи – пошук у потоці даних «заборонених» слів, послідовностей символів («стоп-слів»);
  + Лінгвістичні методи – робота зі словоформами, аналіз усього тексту (наприклад, визначення частоти зустрічальності термінів);
  + Цифрові відбитки - хеш-функції зразків конфіденційних документів;
  + Регулярні вирази – дозволяють знаходити відповідності у формі даних (а не в самих даних), наприклад, номери кредитних карток;
  + Теги – встановлення спеціальних «тегів» на файли, що містять секретну інформацію;
  + Штучний інтелект – самонавчаючийся алгоритм аналізу даних «Western Machine Learning» [23].

Метод аналізу полягає в пошуку в потоці даних послідовності символів («стоп-слів»). У переважній більшості випадків системи підпису налаштовані на пошук кількох слів і частоти зустрічання термінів.

Переваги системи DLP. Стандартні заходи безпеки включають виявлення вторгнень і антивірусне програмне забезпечення. Це механізми, які захищають комп’ютери від внутрішніх і зовнішніх атак.

Додавання рішення DLP до вашої системи кібербезпеки дає вам такі переваги:

1. DLP ефективний для виявлення внутрішніх і зовнішніх загроз. Використовуйте брандмауер, щоб обмежити зовнішній доступ до внутрішньої мережі. Програмне забезпечення DLP може виявляти зовнішні атаки за допомогою антивірусного сканування, щоб знайти троянські програми, встановлені на кінцевих точках, і шкідливе програмне забезпечення, що проникає в мережу компанії через вкладення електронної пошти. Пом’якшить інсайдерські загрози, постійно відстежуючи дані на предмет виявлення порушень даних. Він також шифрує всі дані, скопійовані на USB-пристрій або надіслані в автономному режимі.

2. Рішення DLP запобігають несанкціоновані спроби копіювати або надсилати конфіденційні дані. Класифіковану інформацію можна ідентифікувати за допомогою точного порівняння даних, друку структурних даних, відповідності правил і регулярних виразів, а також концептуальних визначень і ключових слів.

3. Системи DLP дають корпораціям уявлення про те, що відбувається в будівлі. Вони забороняють користувачам подавати конфіденційні дані. За допомогою DLP ви можете побачити, хто намагається надіслати інформацію, і, можливо, зупинити злом, перш ніж це може завдати занадто великої шкоди.

4. Деякі DLP використовують алгоритми машинного навчання для визначення нових конфіденційних даних. Постійний аналіз внутрішнього вмісту допомагає точно визначити всі дані, які необхідно захистити. Ця ж технологія дозволяє виявляти незвичайні запити на доступ і обмін даними між співробітниками. Однак краще використовувати спеціальне рішення для моніторингу активності користувачів або аналізу поведінки та ідентифікації користувачів.

Деякі DLP використовують алгоритми машинного навчання для визначення нових конфіденційних даних [31].

Недоліки системи DLP. Звучить як гарна ідея мати систему DLP, щоб перешкодити порушенням даних, спричинених інсайдерами, а також зовнішніми хакерами. Однак, якщо у вашій компанії є програмне забезпечення DLP, є ризик, що воно може залишити прогалини у вашій корпоративній безпеці. Ви можете відчути, що все захищено, тому не потрібно застосовувати інші заходи безпеки; але це відчуття насправді може бути помилковим відчуттям безпеки.

Використовуючи рішення DLP, необхідно звернути увагу на таке:

1. Система DLP не принесе користі вашій компанії, якщо ви не знаєте, де зберігаються ваші дані. Вам потрібно провести інвентаризацію як секретних, так і несекретних даних. Потім перерахуйте, хто має доступ до секретних даних. Деякі рішення DLP пропонують автоматичне сканування та виявлення конфіденційних даних у корпоративній мережі. Але через специфічні робочі процеси та типи даних у кожній компанії, можливо, краще позначати дані вручну.

2. Система DLP – це бізнес-продукт, а не технологічний проєкт. Після того, як ваша компанія зобов’язується придбати систему DLP, починається важка робота, оскільки рішення DLP важко розгорнути. Щоб зрозуміти, які дані варто відстежувати, вашому ІТ-відділу потрібен вичерпний огляд потоків даних у вашій компанії.

3. Користувачам у вашій мережі призначаються різні привілеї доступу. Вам потрібно перевірити всі рівні привілеїв і переконатися, що ваше рішення DLP здатне відрізнити звичайного користувача від привілейованого.

4. Якщо ваша компанія не витрачає час на визначення своїх стратегій захисту даних і розробку основних технічних і бізнес-вимог, система DLP не буде ефективною. Визначення та впровадження комплексної політики перешкоджання витоку даних займає багато часу. Нечітка політика викликає проблеми з інтеграцією DLP у вашу систему кібербезпеки та додає накладні витрати.

### 1.3 Критерії оцінки DLP-систем як програмного продукту

Запобігання втраті даних (DLP) — це практика виявлення та запобігання злому даних, витоку або небажаного знищення конфіденційних даних. Організації використовують DLP для захисту та захисту своїх даних і дотримання правил.

Організації зазвичай використовують DLP для:

* + Захисту особистої інформації (PII) та дотримання відповідних правил;
  + Захисту інтелектуальної власності має вирішальне значення для організації;
  + Досягнення видимості даних у великих організаціях;
  + Захисту своєї мобільної робочої сили та забезпечення безпеки в середовищі Bring Your Own Device (BYOD);
  + захисту даних у віддалених хмарних системах.

Причини витоку даних*.* Внутрішні загрози – зловмисний інсайдер або зловмисник, який зламає обліковий запис привілейованого користувача, зловживає його дозволами та намагається перемістити дані за межі організації.

Вимагання – метою багатьох кібератак є конфіденційні дані. Зловмисники проникають на периметр безпеки за допомогою таких методів, як фішинг, зловмисне програмне забезпечення або введення коду, і отримують доступ до конфіденційних даних.

Ненавмисне або необережне розкриття. Багато витоків даних відбуваються в результаті того, що співробітники втрачають конфіденційні дані публічно, надають відкритий доступ до даних в Інтернеті або не обмежують доступ відповідно до організаційної політики.

Запобігання витоку даних. Ви можете використовувати стандартні функції безпеки для захисту від втрати та витоку даних. Наприклад, система виявлення вторгнень (IDS) може попереджати про спроби зловмисника отримати доступ до конфіденційних даних. Антивірусне програмне забезпечення може запобігти зловмисникам скомпрометувати чутливі системи. Брандмауер може блокувати доступ будь-якої неавторизованої сторони до систем, які зберігають конфіденційні дані.

Захист даних на ходу. Мережева технологія може аналізувати трафік на предмет конфіденційних даних, надісланих з порушенням політики безпеки.

Безпека кінцевої точки: агенти кінцевої точки можуть контролювати передачу інформації між користувачами, групами користувачів і третіми сторонами. Деякі термінальні системи можуть блокувати спроби зв'язку в реальному часі та надавати зворотній зв'язок користувачам.

Захист даних у використанні. Деякі системи DLP можуть відстежувати та позначати несанкціоновані дії, які користувачі можуть або не можуть робити навмисно під час взаємодії з даними.

Ідентифікація даних. Важливо визначити, захищати дані чи ні. Дані можна визначити як конфіденційні або вручну, використовуючи правила та метадані, або автоматично за допомогою таких методів, як машинне навчання.

Рішення безпеки файлів, такі як брандмауер Imperva File, є важливою частиною стратегії DLP. Ці рішення захищають дані в стані спокою та дані, що використовуються, а також виявляють витік даних на основі файлів.

Компанія Forrester Research розробила чотири основні критерії для оцінки систем DLP.

Перший критерій – багатоканальність. Система DLP має бути комплексною та охоплювати максимальну кількість каналів витоку інформації: електронну пошту, Інтернет та IM, а також моніторинг операцій та потоків файлів в ІТС.

Другий критерій – єдиний менеджмент. Система повинна мати уніфіковані засоби контролю всіх компонентів, що входять до її складу. Головна вимога – керувати всіма частинами системи з одного місця.

Третій критерій – активний захист. Система повинна не тільки фіксувати витоки секретної інформації, але й ефективно блокувати їх у разі потреби.

Четвертий критерій – класифікація інформації за змістом і змістом, категоризація інформації. Методи контролю витоку секретної інформації повинні враховувати такі складові: тип протоколу, тип операції, ідентифікацію користувача тощо.

Виходячи з цих критеріїв, можна зробити висновок, що практично сучасні DLP-системи є великими і складними програмними продуктами. Вибір DLP повинен базуватися на технічних і програмних технологіях, що використовуються в компанії, і задовольняти потреби ІС у каналах витоку інформації в компонентах ІТС [10].

## Висновок до розділу

Розглянуто актуальні задачі безпеки підприємств з розвиненою ІТ-інфраструктурою та чисельністю персоналу, особливості забезпечення безпеки інформаційних ресурсів та побудови інформаційно-телекомунікаційної системи підприємств.

Аналіз технологій DLP, які забезпечують функціонал для протидії витоку секретної інформації та можуть бути впроваджені в ЦПК, з метою мінімізації ризику фінансових та репутаційних втрат.

Проаналізовано функції DLP-систем, на яких рівнях вони захищені, як можна поділити DLP-системи, які основні критерії їх оцінки. Zok-rema, приклад однієї з провідних DLP-систем - Sumantes.

2 МЕТОДИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ DLP ТЕХНОЛОГІЇ

2.1 Системи попередження витоку інформації

Запобігання витоку даних (DLP): Технології запобігання витоку секретної інформації із зовнішньої інформаційної системи, а також обладнання пристроїв для запобігання такого витоку.

Система DLP – це програмний продукт, який блокує несанкціоноване обертання секретної інформації (її витік) з будь-якого оцифрованого каналу зв’язку, враховуючи особливості ІТ-бізнесу.

Канали, якими керує продукт DLP:

* веб-ресурси: загальнодоступні служби електронної пошти, соціальні мережі, форуми, блоги, чати тощо.
* Електронна пошта;
* зовнішні пристрої (USB, CD/DVD, принтери, неавторизовані передавачі Wi-Fi, модеми тощо).
* обмін миттєвими повідомленнями (Telegram, Viber, Slask тощо) [1].

Тому система DLP повинна мати можливість виявляти випадкове або навмисне несанкціоноване використання інформації співробітниками компанії або третіми особами, а не повністю блокувати власні канали. Крім того, на думку вчених, найважливішим критерієм для прийняття рішення про тип DLP є можливість автоматично або вручну аналізувати події та передану інформацію (у реальному часі або так званий постаналіз накопиченого інформаційного файлу). Тому система DLP забезпечує комплексний підхід до запобігання витоку інформації та мінімізації його наслідків: такі події, як відправка конфіденційного документа на принтер, електронну пошту, флешку, відправлення частини конфіденційного документа, можна аналізувати за допомогою миттєвих повідомлень. агент тощо. Також із залученням сучасних DLP-систем можна отримати багато прихованої інформації про своїх колег [38].

Сучасне рішення DLP дозволяє перехоплювати мережевий трафік і на основі бази даних алгоритмів і підписів отримувати передані повідомлення. Повідомлення містять всю доступну мета-інформацію (одержувач, відправник, тема, інші заголовки) та передані файли. Наприклад, система DLP від компанії SearShInform, дозволяє перехоплювати дані на робочому місці, в тому числі використовувані пристрої (ноутбуки і нетбуки), незалежно від того, знаходяться вони в корпоративній мережі чи ні. Система збирає дані та передає їх для аналізу IS, щойно пристрої повертаються до корпоративної мережі.

На рисунку 2.1 наведена схема функціонування DLP – системи.

Рисунок 2.1 – схема функціонування DLP – системи

Кількість даних впливає на вибір типу та сценарію DLP. При використанні DLP виникає питання між вибором між активним і пасивним режимом. В активному режимі DLP «ламає» всіх, хто проходить через мережі передачі даних і блокує несанкціоновану передачу інформації, в пасивному режимі система не блокує, вона лише повідомляє про підозрілі випадки, заносячи інформацію кожного в журнал.

Повні системи DLP також повинні контролювати інші канали. Перш за все, це стосується інтернет-трафіку: Інтернет-пейджери, веб-пошта, соціальні мережі, блоги, форуми, файлообмінники, однорангові мережі, послуги розсилки SMS тощо.

Не всі рішення можуть обробляти повний список потенційних каналів потоку інформації. У більшості західних систем DLP контроль популярних каналів зв'язку на Сході все ще викликає серйозні питання. Це означає, що інформацію, що передається через Інтернет-месенджери, можна аналізувати лише деякими рішеннями DLP.

Розслідування справи є необхідною частиною будь-якої системи захисту від витоку інформації. Тому часто доводиться не тільки знайти та заблокувати витік, а й провести службове розслідування у кожному конкретному випадку. Це означає, що таке розслідування може включати як аналіз ідентифікованої секретної інформації, так і ретроспективну перевірку активності користувачів. На жаль, багато DLP не тільки не дозволяють легко перехоплювати перехоплені дані, але й не зберігають заблоковану інформацію, що вкрай незручно та непрактично. У цьому випадку неможливо зрозуміти, що насправді було заблоковано, оскільки навіть сама система технології DLP може помилятися у виборі обраної інформації.

Фактично є можливість розділити на хостові DLP, що встановлюються на кінцеві точки мережі – настільні комп'ютери і ноутбуки, мережеві та змішані. Чисто хостові DLP, тобто контролюючі як зовнішні пристрої та принтери, так і всі мережеві канали витоку, останнім часом набувають все більшого поширення. Їх безперечні переваги – простота і відносна дешевизна, зате хостові DLP мають список важливих недоліків: невисока продуктивність, масштабність, висока ціна наступної підтримки та вимоги до характеристик кінцевих точок мережі. Варто сказати, що практика показує, що такі системи DLP варто використовувати у організаціях незначного розміру.

До того ж, кожного разу, коли є пошта або файл для надсилання від колеги, DLP перевірить усі умови та обмеження, які визначені адміністратором і будуть або заблоковані або дозволені поштою. Система буде визначати витік даних на базі трьох параметрів: обмеження часу та розширення та ключові слова. Система також буде генерувати пошту для адміністрування та створення вимог.

### 2.2 Структурна інформаційна безпека підприємства

Статус інформаційної безпеки компанії - це здатність і здатність компанії протистояти будь-яким спробам завдати шкоди її законним інтересам.

Завданнями системи інформаційної безпеки є:

* віднесення інформації до категорії обмеженого доступу
* протидіяти витоку такої інформації;
* прогнозування, своєчасне виявлення та усунення загроз безпеці інформації компанії; причини та умови, що сприяють заподіянню економічної, матеріальної та моральної шкоди, зміні нормального функціонування та розвитку;
* створення механізму та умов для оперативного реагування на загрози інформаційній безпеці;
* ефективне припинення посягань на інформаційні ресурси компанії на основі правових, організаційних та інженерних заходів та заходів безпеки.

Об'єктами безпеки є:

* відомості про персонал (адреса, штат);
* інформація про використовувані технології;
* Інформація для споживачів;
* інформація про проекти;
* інформаційні ресурси (інформація з обмеженим доступом, що становить комерційну таємницю, інша секретна інформація, що надається у вигляді документів і файлів, незалежно від форми та виду подання)

Структурно безпека інформації компанії складається з: безпеки інформаційних ресурсів, безпеки інформаційної інфраструктури та безпеки «інформаційного поля» компанії.

Компанія займається формуванням інформаційних ресурсів, використовуючи інформаційні технології та комунікаційні методи, які забезпечують обробку, зберігання та передачу інформації.

Системна безпека – це стан безпеки комп’ютерів компанії, комп’ютерних систем і мереж і телекомунікаційних мереж, що забезпечує цілісність і доступність інформації, що в них обробляється (зберігається або розповсюджується). [12]

Основними завданнями для забезпечення безпеки інформаційних ресурсів є:

* запобігання витоку інформації про клієнтів;
* запобігання витоку проектної інформації;
* організація та контроль доступу працівників до необхідних інформаційних ресурсів відповідно до потреб виробництва або посад (старші керівники та керівники відповідних підрозділів).

Найбільш суттєвими загрозами безпеці інформаційних ресурсів є втрата або втрата інформаційних ресурсів (у тому числі інформації про клієнтів і проекти).

Основними загрозами інформаційної безпеки компаній є:

* Природні, техногенні та соціальні несприятливі явища;
* збої, знищення/пошкодження програмного та апаратного забезпечення;
* терористи та кримінальні елементи;
* залежність від постачальників / постачальників / партнерів / клієнтів;
* працівники, які погрожують ІБ, використовуючи законно надані права та повноваження (внутрішні порушники ІБ);
* Співробітники, які здійснюють погрози ІБ без прав і повноважень, передбачених законодавством, а також суб'єкти, які не є працівниками компанії.

Основними організаційно-технічними заходами для забезпечення інформаційної безпеки є:

* постійний і повний аналіз інформаційної системи для виявлення вразливих місць інформаційних активів компанії;
* своєчасне виявлення проблем, які потенційно можуть вплинути на безпеку інформації компанії, коригування моделей загроз та порушників;
* розробка та впровадження заходів захисту відповідно до аналізу ризиків інтелектуальної власності та сучасного стану КСЗІ;
* контроль ефективності вжитих заходів захисту;
* персоніфікація та розподіл ролей та відповідальності між працівниками;
* проводити аудит ІБ з урахуванням загроз, ризиків і порушень безпеки ІБ;
* планові перевірки ризиків з використанням інформації про технологічні та організаційні зміни в інформаційній безпеці бізнесу та компанії;
* вести облік дій та подій, які можуть вплинути на ефективність інтелектуальної власності компанії;
* вносити зміни до планів безпеки для забезпечення реалізації результатів контрольно-моніторингової діяльності системи.

## 2.3 Структура інформаційно-телекомунікаційної системи типового підприємства

Підприємства ІТС, що забезпечують функціонування та застосування всіх бізнес-процесів і завдань, можна представити у вигляді ієрархії таких основних рівнів:

* фізичні (лінії зв'язку, апаратні методи тощо);
* мережеве обладнання (мережні апаратні методи: маршрутизатори, комутатори, концентратори тощо);
* мережеві додаткові програми та послуги;
* операційні системи;
* системи управління базами даних.

Основою інформаційної системи є база даних первинних документів, до неї також входять сервери обробки та зберігання даних із серверами додатків, що реалізують такі компоненти ІТС, як системи електронної пошти, системи управління та управління проектами, системи контролю версій, бази знань.

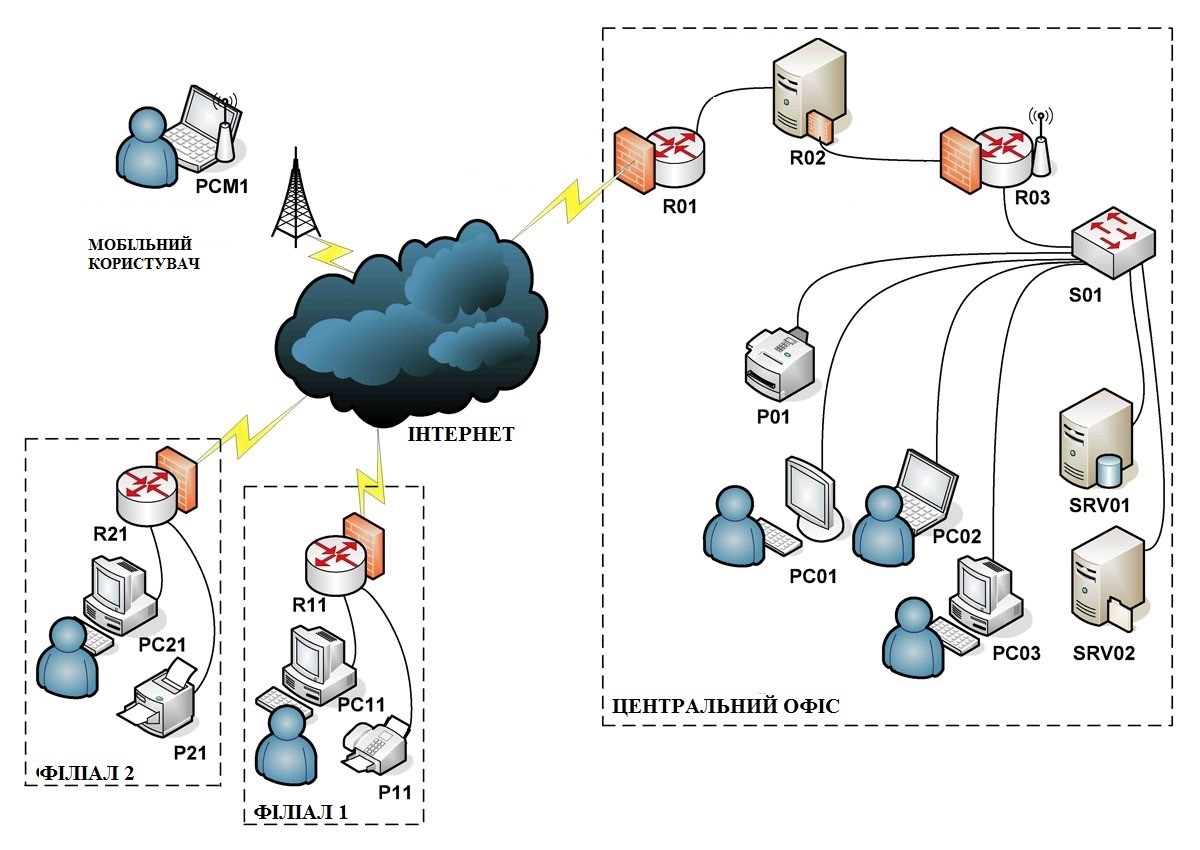


Рисунок 2.1 - Загальна схема ІТС типового підприємства

Вся інформація циркулююча на підприємстві пов’язана із клієнтами, бізнес процесами підприємства, персональними даними є секретною. Доступ до інформації працівники отримують відповідно до посади та виробничих функцій.

Інформаційні потоки в межах ІТС підприємства відбуваються між працівниками та клієнтами, та дійсно із доступом до ресурсів та виробничим потребам. [18]

## 2.4 Джерела загроз безпеці ІТС підприємств

Криміногенна ситуація в країні, наявність жорсткої конкуренції та потужних фінансових потоків і технічного оснащення підприємств дає підстави для зростання ризиків інформаційної безпеки комерційних підприємств. Звідси визначення та прогнозування можливих загроз та усвідомлення їх небезпеки необхідні для обґрунтування, вибору та реалізації захисних заходів.

Під поняттям загрози розуміють потенційно можливі або реальні дії злого умислу чи конкурентів, які можуть завдати матеріальної чи моральної шкоди.

Загроза інформаційній безпеці ІВ - сукупність умов і факторів, що створюють ризик несанкціонованого доступу до інформації, що циркулює в автоматизованій системі, а також можливі наслідки дій порушника на ІП підприємства, не перешкоджаючи, до погіршення. зазначених якісних характеристик функціонування ІВ або порушення його ефективності, а також спотворення та витоку інформації. [25]

Загроза: будь-яка обставина або подія, яка може призвести до порушення політики інформаційної безпеки та/або пошкодження інтелектуальної власності.

Загрози та їх джерела (включаючи зловмисників), методи та прийоми захисту, а також підходи до оцінки ефективності можна визначити за рівнем ІТС. Тому ефективна робота ІТС та інформаційна безпека вимагає розподілу інформації за рівнями інформаційної інфраструктури.

Рівні інформаційної інфраструктури:

* операційні системи;
* мережа додаткових програм і сервісів;
* системи управління базами даних;
* фізичні (лінії зв'язку, апаратні методи тощо);
* мережеве обладнання (мережні апаратні методи: маршрутизатори, комутатори, концентратори тощо);
* бізнес-процеси організації.

Джерела загроз на фізичному, мережевому та плагіновому рівні:

* зовнішні джерела загроз: розповсюджувачі вірусів та інших шкідливих програм, хакери та інші, хто виконує НСД;
* внутрішні джерела загроз: люди, які здійснюють загрози в межах вашої юрисдикції та за її межами (персонал, який має права доступу до комп’ютера, включаючи мережу, адміністратори мережевих програм тощо);
* комбіновані джерела загроз: зовнішні та внутрішні, що діють разом та/або узгоджено.

Джерела загроз на рівні операційних систем, систем управління базами даних, технологічних процесів:

* внутрішні, щоб вони усвідомлювали загрози в межах своїх повноважень і поза ними (адміністратори ОС, адміністратори СУБД, адміністратори ІС тощо);
* комбіновані джерела загроз: зовнішні та внутрішні, що діють у змові.

Загрози Je-rela на рівні бізнес-процесів:

* внутрішні джерела, які здійснюють загрози в межах своєї компетенції та поза ними (уповноважені користувачі та оператори АБС, представники керівництва організації тощо);
* Змішані джерела загроз: зовнішні (наприклад, конкуренти) і внутрішні, змовні.

Пріоритетом успішної роботи ІТ-компанії, як зазначалося вище, є підтримка стабільної роботи ІТС та забезпечення безпеки інформаційних потоків в обігу.

На рисунку 2.2 представлені основні загрози, які впливають на конфіденційність, цілісність та доступність інформаційних ресурсів.

Поняття конфіденційності, цілісності, доступності наведено згідно з НД ТЗІ 1.1-003-99 Термінологія у сфері захисту інформації в комп’ютерних системах від несанкціонованого доступу.

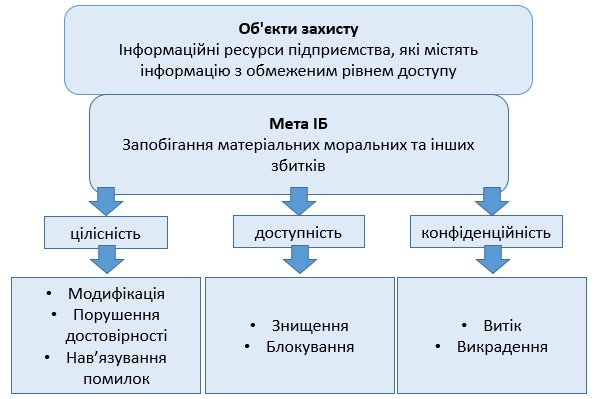
.

Рисунок 2.2– Базові загрози безпеці інформаційних ресурсів

Загрози порушення конфіденційності включають крадіжки (копіювання) та витоки. Основними видами атак, спрямованими на порушення конфіденційності, є пасивне прослуховування та перехоплення в каналах зв’язку, незаконне використання прав, крадіжка ключової інформації.

Витоки/втрати інформації підривають довіру до компаній і завдають величезних збитків. За прогнозами аналітиків, у найближчі кілька років світовий бізнес-сектор зазнає збитків у розмірі близько 1 трлн доларів. щорічно через витік конфіденційних даних.

Загрози доступності даних виникають, коли об’єкт (користувач або процес) не має доступу до законодавчо визначених служб або ресурсів. Ця загроза здійснюється шляхом захоплення ресурсів, блокування ліній зв'язку несанкціонованими об'єктами в результаті передачі їм вашої інформації або виключення необхідної інформації з системи. Ця загроза може призвести до ненадійності або низької якості обслуговування в системі і, таким чином, потенційно вплинути на надійність та своєчасність доставки платіжних документів.

Відповідно до вимог СІУ НБУ 65.1 ISMS 1.0:2010 інформаційна безпека забезпечує збереження конфіденційності, цілісності та доступності інформації та може враховувати інші властивості, такі як надійність, спостережливість, визначеність та надійність [30].

На рисунку 2.3 наведена модель реалізації загроз з урахуванням джерел загроз, вразливостей та методів загроз інформаційній безпеці.

Загрози інформаційним ресурсам проявляються у вигляді:

* розкриття секретної інформації;
* витоки секретної інформації за допомогою технічних методів для забезпечення різного характеру та продуктивності виробничої діяльності;
* несанкціонований доступ до захищеної інформації з боку конкуруючих організацій та злочинних груп.

Погрози інформаційним ресурсам можуть бути:

* шляхом неофіційного доступу та видалення секретної інформації;
* підкуп осіб, які працюють у банку або структурах, безпосередньо пов'язаних з його діяльністю;
* шляхом перехоплення інформації, що циркулює в інструментах і системах;



Рисунок 2.3 – Модель реалізації загроз

* комунікаційно-обчислювальна техніка за допомогою технічних засобів розвідки та пошуку інформації, несанкціонованого доступу до інформації та навмисних програмно-математичних дій з нею в процесі обробки та зберігання;
* шляхом підслуховування конфіденційних переговорів, що ведуться в офісних приміщеннях, службовому та особистому транспорті тощо;
* через переговорні процеси між компанією та іноземними чи вітчизняними фірмами, використовуючи необережне поводження з інформацією;
* через окремих працівників підприємства, які прагнуть отримати понад свою зарплату, дохід або мають інші корисливі чи особисті інтереси.

За джерелом загрози безпеці комерційної установи є:

* загрози з боку конкурентів, тобто вітчизняних та іноземних компаній, які прагнуть зміцнити свої позиції на відповідному ринку шляхом застосування заходів недобросовісної конкуренції, таких як економічний шпигунство, залучення висококваліфікованих працівників, дискредитація опонента в очах партнерів та держави;
* погрози з боку кримінальних структур та окремих злочинців, які прагнуть досягти власних цілей, що суперечать інтересам конкретного підприємства, наприклад, захоплення контролю над ним, розкрадання майна, заподіяння інших збитків;
* Погрози з боку нелояльних співробітників компанії, які свідомо завдають шкоди для досягнення власних цілей, наприклад, покращення фінансового становища, кар’єрного зростання, помста роботодавцю за реальні чи уявні образи тощо.

За типами можливих джерел загроз ІБ виділяють наступні класи загроз:

* загрози, пов'язані з навмисними або ненавмисними діями осіб, які мають доступ до IP, у тому числі користувачів IP, які реалізують загрози безпосередньо в IP (внутрішній порушник);
* загрози, пов'язані з навмисними або ненавмисними діями осіб, які не мають доступу до IP, які здійснюють загрози з боку зовнішніх мереж загального користування та (або) міжнародних мереж обміну інформацією (зовнішній зловмисник).

За типами несанкціонованих дій з інформаційними ресурсами виділяють наступні класи загроз:

* загрози, що порушують конфіденційність ІВ (копіювання чи несанкціоноване поширення), реалізація яких не має прямого впливу на зміст інформації;
* загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на зміст інформації, що призводить до зміни ІВ або їх знищення;
* загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на програмне забезпечення або апаратно-програмні елементи IP, що призводить до блокування IP.

На думку вітчизняних та зарубіжних дослідників, персонал є важливим внутрішнім джерелом ризику прийняття помилкових рішень і неправомірної поведінки, у тому числі у зв'язку з діями інших осіб та організацій щодо примусу працівників до злочинної діяльності. При цьому можливі спроби ввести в штат представників злочинних та інших недружніх підприємству організацій.

## 

## 2.5 Аналіз загроз джерелам інформаційних ресурсів ІТС компаній

У кваліфікаційній роботі створення моделі загроз буде реалізовано з урахуванням найбільш істотної загрози витоку інформаційних ресурсів у компанії: навмисних чи ненавмисних дій внутрішніх порушників.

У таблиці 6 представлена модель загроз безпеці інформаційних ресурсів, джерелом яких є навмисні та ненавмисні дії персоналу.

Функція ймовірності реалізації певної загрози, вид і величина збитку визначає ризик для безпеки інформаційних ресурсів підприємства.

Як аналіз ризиків визначається процес виявлення загроз інформаційної безпеки та їх характеристик, слабких місць ІСІС (відомих і прийнятних), оцінки потенційних втрат від реалізації загроз та ступеня їх прийнятності для функціонування АС.

В таблиці 7 наведена модель загроз безпеці інформаційних ресурсів із впровадження системи захисту від витоків на основі DLP.

Під загрозою розуміють її можливий вплив на безпеку інформаційних ресурсів підприємства, що може мати негативні наслідки.

На рисунку 2.3 наведено порівняльний опис ймовірностей загроз безпеці інформаційних ресурсів від ненавмисних дій внутрішніх порушників, до та після впровадження системи DLP, що відображає ефективність системи протидії витоку інформації, класифікованої на основі DLP [14].



Рисунок 2.3 – Порівняльний аналіз ймовірностей реалізації загроз від ненавмисних дій внутрішніх порушників

За результатами порівняльного аналізу суттєво знижується ймовірність загрози ненавмисних дій персоналу внаслідок недбалості/недбалості, а також помилок при обробці інформації.

На рисунку 2.4 наведено порівняльний опис ймовірностей загроз безпеці інформаційних ресурсів від навмисних дій внутрішніх зловмисників, до та після впровадження системи DLP, що відображає ефективність системи боротьби з витоком секретної інформації. на основі DLP.

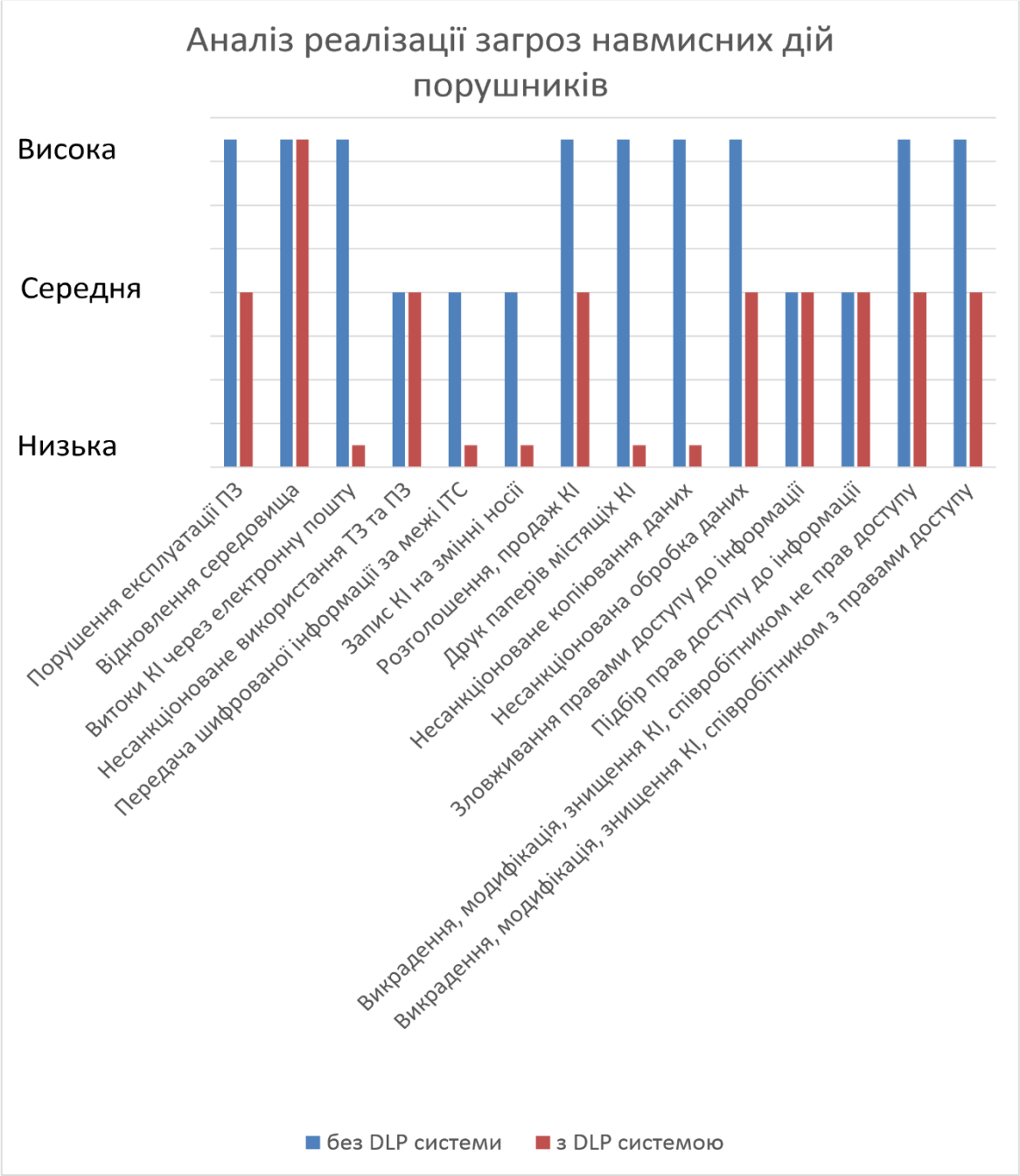


Рисунок 2.4 *–* Порівняльний аналіз ймовірностей реалізації загроз від навмисних дій внутрішніх порушників

Результати порівняльного аналізу відображають суттєве зниження ймовірності реалізації загроз навмисних дій персоналу за такими напрямками:

* передача КІ за допомогою електронної пошти;
* передача зашифрованої інформації у зовнішню мережу;
* передача незашифрованої інформації у зовнішню мережу;
* запис КІ на знімний носій;
* друк документів, що містять КІ;
* шахрайське копіювання даних [24];

Також зменшується ймовірність виникнення загроз, пов’язаних із зміною, знищенням, незаконною обробкою інформації [40].

Висновок до розділу

У другому розділі розглядається структура існуючих DLP-рішень, методи захисту інформації, засновані на використанні цих рішень та їх вплив на модель інформаційної безпеки в ІТС підприємства.

Розглянуто та проаналізовано загрози безпеці в ІТС типового підприємства та проаналізовано вплив використання моделей ІС на основі використання DLP-систем на стан інформаційної безпеки.

Проаналізовано провідні DLP-системи, їх компоненти, методи використання, плюси та мінуси.

Розглянуті моделі підтримки ІС позитивно впливають на стан інформаційної безпеки в ІТС підприємства.

Система DLP розглядається як частина CPC, яка спрямована на мінімізацію ризиків прямих і непрямих фінансових наслідків витоку секретної інформації.

# 3 ВПРОВАДЖЕННЯ МЕТОДУ АPІ HООKІNG

3.1 API Hooking

Підключення API Hooking охоплює цілий ряд методів для зміни або покращення поведінки операційної системи, програми чи інших програмних компонентів шляхом перехоплення викликів функцій API, повідомлень або подій, що передаються між програмними компонентами. Код, який обробляє таке перехоплення, називається хуком.

Деякі з програмних додатків, які використовують хуки, — це інструменти для програмування, захисту від шкідливих програм, рішень із захисту додатків та інструментів моніторингу. Шкідливе програмне забезпечення також часто використовує хуки; наприклад, щоб приховати зі списку запущених процесів або перехопити події натискання клавіш, щоб вкрасти конфіденційні дані, такі як паролі, дані кредитної картки тощо.

Існує два основних способи змінити поведінку виконуваного файлу:

* за допомогою підходу до модифікації джерела, який передбачає модифікацію виконуваного двійкового файлу перед запуском програми за допомогою зворотного проектування та виправлення. Для захисту від цього використовується підписання виконуваного файлу, запобігаючи завантаженню коду, який неправильно підписаний.
* через модифікацію часу виконання, яка реалізується API операційної системи. Microsoft Windows надає відповідні джгути для підключення діалогових вікон, кнопок, меню, подій клавіатури, миші та різних системних викликів.

Хуки API можна розділити на такі типи:

* Локальні хуки: вони впливають лише на конкретні програми.
* Глобальні хуки: вони впливають на всі системні процеси.

У цьому розділі ми розглянемо техніку API Hooking для Windows, яка належить до локального типу nf виконується за допомогою модифікації середовища виконання.

Операційна система Windows або практично будь-яка інша ОС складається з різноманітних розділених програмних компонентів, які працюють в тандемі, щоб забезпечити роботу кінцевого користувача. Багато разів програмне забезпечення сторонніх розробників також покладається на ці компоненти для функціонування. Щоб дозволити цим різним компонентам коректно взаємодіяти один з одним, не викликаючи конфліктів, використовуються інтерфейси прикладного програмування (або скорочено API). Коли програмному забезпеченню A потрібна певна функціональність, яку пропонує компонент ОС B, вона викликає одну з доступних функцій B, визначену в його API.

У Windows основний набір функцій, які ОС робить доступними для програмних компонентів, обробляється через Windows API, також відомий як WinAPI. WinAPI надає доступ до базових служб, таких як файлова система, процеси та потоки; і до служб вищого рівня, таких як керування інтерфейсом користувача та мережа (наприклад, NetBIOS і RPC)

Яким би потужним не був WinAPI, іноді розробники хочуть змінити потік коду його функцій, щоб розширити або змінити функціональність програмного забезпечення. Наприклад, коли я пишу цю статтю і натискаю клавіші на клавіатурі, ОС генерує повідомлення WM\_KEYDOWN і доставляє їх за допомогою API до мого текстового редактора для обробки. Але що, якби я встановив програмне забезпечення третьої сторони, яке перевіряє орфографію мого введеного тексту під час введення? Програмне забезпечення повинно було б отримати повідомлення, призначене для мого текстового редактора, обробити його, а потім передати результат процесів текстовому редактору, виконуючи свого роду людину посередині.

Це називається підключенням — процесом, за допомогою якого програма перехоплює виклик API між двома іншими програмами. У наведеному вище прикладі функція перехоплення (звана процедурою перехоплення) змінила дані, передані одержувачу (текстовому редактору), але це не завжди так.

Щоб зробити доступною цю поведінку, Windows надає розробникам механізм перехоплення подій, повідомлень і певних викликів API, які називаються хуками. Для кожного гачка Windows обробляє окремий ланцюжок гачків, перелічуючи покажчики на всі пов’язані з ним процедури перехоплення. Щоб використовувати хук, розробники викликають функцію WinAPI SetWindowsHookEX. Коли відбувається подія, яка відстежується за допомогою хука, наприклад, вищезгадана подія натискання клавіші, ОС викликає першу процедуру в ланцюжку перехоплення. Ця процедура виконується, а потім або викликає наступну процедуру в ланцюжку гачка, або розриває її. Зверніть увагу, що деякі гачки дозволяють ланцюжку лише відстежувати потік даних, але не змінювати його. Ці гачки також не дозволяють підлеглим процедурам розірвати ланцюг.

Хуки можуть бути глобальними, тобто застосовуватися до всіх релевантних подій у межах свого робочого столу, або специфічними для потоку. Якщо гачок глобальний, підключена процедура має зберігатися в окремому файлі DLL, щоб різні потоки могли спільно використовувати його.

Повинна бути можливість ідентифікувати та класифікувати дані відповідно до набору правил/політик, а також мати можливість адаптувати та застосовувати ці правила відповідно до різних випадків. Дії, зроблені для кожного файлу, також мають бути записані, а користувач повинен пояснити, чому було зроблено цю дію. Використання простого способу визначення правил з використанням чорних і білих списків, файлів і файлів, що містять попередньо визначений підпис, дозволить можливу інтеграцію з рішеннями, подібними до тих, що були оцінені в розділі 2. Ідея полягає в тому, що існуючі рішення можуть надавати інформацію про те, які файли слід розглянути. конфіденційно.

Щоб програми отримували доступ до даних, збережених на таких носіях, як жорсткий диск, CD/DVD або знімний носій, програми запитують дані через операційну систему. Це також стосується зберігання або передачі даних між носіями, наприклад надсилання файлів по мережі або копіювання файлів з жорсткого диска на USB-накопичувач. Розмістивши рівень перевірки між програмою та операційною системою, ви можете контролювати, хто і що матиме доступ до яких даних.

Один із способів досягти цього – перехопити виклики функцій в операційній системі програми та перенаправити їх на іншу функцію. Ця техніка також відома як прив’язка API, з’єднання API, також називається відстеженням системних викликів або інтерфейсом системного виклику.

Підключення API є досить вимогливим і ризикованим, якщо ви помилитеся. Після підключення API код повинен обробляти всі виклики функцій цього API, будь-які помилки можуть призвести до збою програми або навіть системного збою, наприклад, BSOD, синій екран смерті. Microsoft Research розробила фреймворк для Windows, щоб зробити підключення API простішим і безпечнішим. Ця структура відома як Detours [10] і доступна у двох версіях: Express та Professional. Є обмеження: у першій версії можна, наприклад, обмежити підтримку процесорів. Перша версія працює лише для архітектури x86. Тут був використаний аналог з відкритим кодом для Detours, а саме фреймворк EasyHook, який спирається на концепцію Detours і продовжує її вдосконалювати.

Виявлення та підключення до API Windows, пов’язаних з керуванням файлами, за допомогою платформи EasyHook, реалізовано такі функції:

* SopuFile
* Среаtefilе
* Видалити файл
* MoveFile
* ReadFile
* ReplaseFile
* WriteFile

Список файлів і каталогів, які слід заблокувати та дозволити, визначено заздалегідь. Також визначено список магічних чисел і підписів, які підлягають блокуванню. Ми змогли запобігти доступу до файлів, які були заблоковані, не внесені в білий список або містять заблокований магічний номер чи підпис через будь-який із зазначених API. [6]

Підключення API було вичерпно висвітлено протягом останнього десятиліття. Це важлива тема у сфері програмного забезпечення, зворотного проектування та всього, що пов’язано з пам’яттю ОС. У парі з ін’єкцією процесу підключення може або дати уявлення про те, що виконує виконуваний файл, або зловмисно перехопити та змінити будь-які виклики, зроблені до WinAPI.

Цей метод просто намагається замінити перші кілька байтів експортованої функції з DLL, завантаженої та використаної цільовим виконуваним файлом/процесом. Перезапис певним чином перейде до місця в пам’яті всередині процесу, яким ви керуєте. Звідти вам вирішувати, що станеться з перехопленим викликом. Ви можете, наприклад, підключити CreateFile, і як тільки виклик буде перехоплений, просто відкиньте його та невдало повернете. Ефектом у цьому прикладі буде відмова у доступі до створення файлів або, якщо більш цільовий, заборона доступу лише до певних файлів.

## 3.2 Використання АPІ Hооkіng

АPІ Hооkіng забезпечує:

1. Можливість контролю вхідного http-трафіку й “підміна” небажаного контенту на той, котрий ми приймаємо.

2. Можливість застосування логування інформацію у випадку копіювання будь-яких файлів з підконтрольованої папки.

1. Можливість застосування певних модифікацій коду в проєкті, початковий код якого було певним чином втрачено.

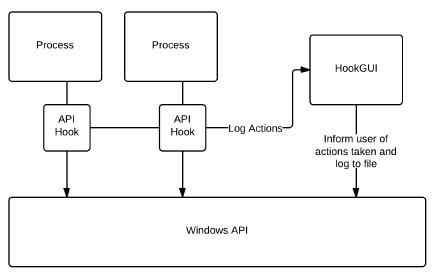
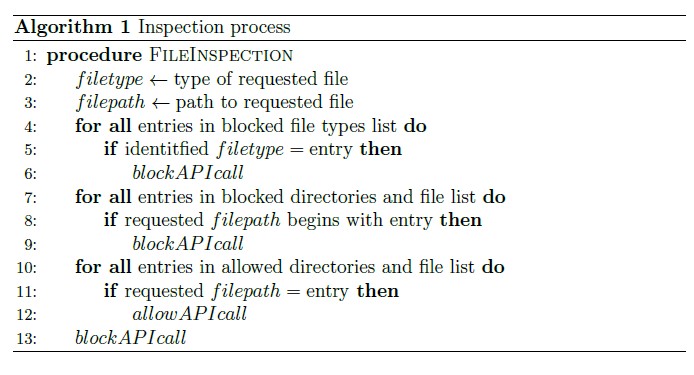


Рисунок 3.1 – Ілюстрація реалізованого рішення

## 3.3 Види АPІ Hооkіng

Перехоплення перед запуском. Це виконується фізичним модулем (зазвичай файлами .exe або .dll), коли ми використовуємо функцію, яку ми намагаємося перехопити та перенаправити. Як правило, існує три варіанти, які можна використовувати для досягнення бажаного результату.

Перший — знайти точку входу до цільової функції та змінити чи переписати код. Цей метод обмежений розміром самої функції. Однак у цьому випадку ми можемо динамічно завантажувати певні модулі за допомогою LoadLiber API. Функцію ядра (kernel32.dll) можна використовувати майже у всіх випадках, оскільки кожен процес у Windows має власну копію цього модуля. Перевага також, коли ми знаємо, в якій операційній системі ми будемо змінювати модуль. У цьому випадку ми можемо використовувати прямі покажчики на LoadLiber API. Їх можна використовувати, оскільки основна адреса модуля в пам'яті є статичною. Ви також можете використовувати відстеження поведінки для завантажених динамічних модулів. У цьому випадку частина ініціалізації починається відразу після завантаження пам’яті. Також немає обмежень щодо ініціалізованих частин у нових модулях.

Друга можливість полягає в тому, що ми використовуємо розширення для перевизначення або перенаправлення функції в модулі. Ви повинні вибрати перші 5 байтів і замінити їх або переписати IAT. У першому випадку відбудеться перенаправлення коду, який виконується в нашому коді. Коли викликається функція, яка змінює регістр IAT, наш код запускається відразу після цього виклику. Однак розширити модуль непросто, тому що потрібно звернути увагу на DLL.

Третій спосіб — повністю замінити весь модуль. Це означає, що вам доведеться створити власну версію модуля, яка зможе завантажити оригінал і викликати оригінальні функції, які більше не потрібні. Однак нові функції, які були додані з новою версією модуля, будуть абсолютно новими. Цей метод не дуже ефективний для великих модулів, оскільки вимагає багато часу та ресурсів для експорту.

Перехоплення під час роботи. Перехоплення перед запуском в першу чергу є спеціалізованим, дуже конкретним і націленим на конкретні програми або модулі. Якщо ви перевизначите функцію в kernel32.dll або ntdll.dll, у нас буде великий шанс замінити цю функцію в усіх процесах, які будуть запущені пізніше. Однак ці процедури дуже складні, оскільки ви повинні контролювати точність і покращення коду для нової функції та всього модуля. Однак головна проблема полягає в тому, що процес, який буде запущений в майбутньому, буде перехоплений (тобто необхідно буде перезапустити всі процеси). Ще однією проблемою є складність доступу до системних файлів. Набагато краще виглядає вирішення процесів перехоплення під час його перебігу. Цей метод вимагає більше інформації та знань, але результат є найкращим. Перехоплення в процесі можливе лише для процесу, до якого ми маємо доступ до «запису» в пам'яті. Для запису можна використовувати функцію API WriterProcessMemor.

## 3.4 Методи встановлення АPІ Hооkіng

Різні типи методів можуть бути використані для встановлення різних типів методик та використання різних технологій та застосувань.

Одним із цих методів є використання функції SetWookHex. Наш метод простий, але обмежений. Метод перехоплення лише функцій, які зазвичай пов’язані з програмним підприємством (наприклад, перехоплення подій, які можна направити на програму, натискання миші, щоб написати комп’ютер або писати в програмі). Продажом цього методу є можливість встановлення та використання загального перехоплення (наприклад, можна перехопити вхід усіх програм у програмі).

Використання напрямку повторного імпорту у відділі імпорту DLL. Цей метод узгоджується з можливістю модуляції імпортного відділу. Остання кількість усіх використаних модулів у першу чергу. Існують також напрямки пам’яті для експортованих функцій цим модулем. Застосуйте метод, що відповідає напряму нашого модуля, морем переваг для нас. Після застосування цих дій жест переноситься у вказаний напрямок.

Третя форма — це використання розділу реєстру HKEU\_LOCAL\_MASHINE \ Software \ Software \ Microsoft \ Windows \ Windows \ SurventVersion \ Windows \ AppInit\_Dlls. У реєстрі необхідно зареєструвати DLL-маршрут, але праворуч тільки користувача з правами адміністратора. Цей метод простий і ефективний, якщо програма не використовує kernel32.dll (вона повинна мати можливість почати використовувати функцію LoadLiber).

Ін'єкційний метод. Цей метод можливий завдяки функції ThreadStart, яку можна використовувати для створення функції CreateThread, компанії, схожої на функцію LoadLibar. Це перший, хто вказує метод LoadLibar як аргумент для створення hilo.

Нижче наведено алгоритм використання DLL-ін’єкції:

* Знайдіть функцію LoadLiber за допомогою Kernel32.dll для hilo, в якій ми встановлюємо вхідну лінзу DLL.
* Призначити пам'ять для запису аргументів у цій функції.
* Ви створюєте послідовність. Як функцію ThreadStart ми вказуємо функцію LoadLibar та її аргумент.
* Зараз ви завантажуєте та завантажуєте бібліотеку.
* Бібліотека призначення розташована в просторі напрямків третього напрямку.

У цьому випадку метод DllMain позначається індикатором PROCESS\_ATTASH для завантаження DLL. Це саме те місце, де ми можемо встановити перехоплення для потрібних нам функцій.

Щоб продовжити, опишемо більш детально процес встановлення сприйняття:

* Необхідно знайти напрямок функції перехоплювача llamada planamos. Для цього можна використовувати MesageBox і user32.dll.
* Захистіть перші байти функції в нашій області пам'яті.
* У розташування байтів захисної функції вставляємо елемент керування JUMP-машиною для напрямку товарної функції. Для правильного застосування необхідно переконатися, що компанія має функцію монети з компанією вихідної функції. Кажуть, всі параметри, а також значення риторики і правил ламади повинні точно відповідати вихідній функції.

Останній крок полягає в наступному. Коли потік викликає функцію, яку ми плануємо захопити, команда JUMP, яка була раніше вставлена замість першого байту функції, перенаправить потік до функції, яку ми замінюємо. На цьому етапі ми зможемо виконати довільний код.

Перехоплення викликів Win32 API не завжди було легким завданням. Термін перехоплення (перехоплення) є основним методом отримання контролю над певними фрагментами, або фрагментом коду програми. Перехоплення забезпечує простий механізм, який може змінити поведінку операційної системи, а також поведінку програм, які запускаються без доступу до вихідного коду.

Багато сучасних систем звертають увагу на здатність використовувати існуючі програми Windows певними «шпигунськими» методами. Ключова мета і завдання перехоплення полягає не тільки в просуванні більш розширеної функціональності, але й у реалізації коду інверсії для досягнення певних цілей.

Сучасні операційні системи забезпечують складні механізми виділення адресного простору кожного процесу. Ці архітектури захищають пам'ять, тому жодна з програм не може пошкодити або змінити адресний простір іншого процесу.

Ось деякі з переваг програм моніторингу та перехоплення:

* Моніторинг функцій API.
* Можливість керувати викликами API надзвичайно корисна і дозволяє відстежувати приховані дії, які можуть відбуватися під час виклику API. Це дозволяє ретельно перевірити параметри функцій, а також звіти про проблеми, які зазвичай можна ігнорувати. Іноді може бути корисно мати можливість керувати функціями API, пов’язаними з пам’яттю, щоб усунути витрати ресурсів.
* Налагодження реверс-інжинірингу.
* На додаток до стандартних методів налагодження API, перехоплення має репутацію одного з найпопулярніших механізмів налагодження. Багато розробників використовують методи перехоплення та моніторингу API для визначення різних компонентів та їх взаємозв’язків. Перехоплення API — це дуже складний спосіб отримати інформацію про двійковий виконуваний файл.
* Подивіться всередину операційної системи.
* Часто розробники хочуть зрозуміти операційну систему, її структуру та архітектуру на досить глибокому рівні. Перехоплення та моніторинг також є дуже корисним методом декодування недокументованих або погано задокументованих API.
* Розширення запропонованої функціональності.

Це робиться шляхом вбудовування спеціальних модулів у зовнішні програми Windows. Перевстановлення звичайного коду для ін’єкційних гачків може забезпечити простий спосіб змінити та розширити функціональність існуючого модуля. Наприклад, багато продуктів іноді не відповідають певним вимогам безпеки і повинні бути налаштовані відповідно до ваших конкретних потреб. Перехоплення та моніторинг перехоплювачів дозволяють розробникам додавати складні функції API початкової попередньої та постобробної обробки. Ця здатність надзвичайно корисна для зміни поведінки вже скомпільованого коду. [40]

## 3.5 Функціональні вимоги до системи перехоплення та моніторингу

Перед впровадженням будь-якої системи перехоплення API необхідно прийняти кілька важливих рішень. По-перше, вам потрібно визначити, чи потрібно перехоплювати й відстежувати одну програму чи використовувати системний механізм. Наприклад, якщо ви хочете відстежувати лише одну програму, вам не потрібно встановлювати загальносистемну систему перехоплення та моніторингу, але якщо ваша робота полягає в тому, щоб відстежувати всі виклики до TerminateProcess або WritProcessMemory, єдиний спосіб зробити це – це мати систему інструментів моніторингу. моніторинг перехоплювача.

Зазвичай система перехоплення складається щонайменше з двох частин: сервера перехоплення контролера. Сервер перехоплення відповідає за знайомство контролера з цільовими процесами у відповідний момент. Він також керує водієм і додатково може отримувати інформацію від водія про його діяльність, в той час як модуль драйвера здійснює фактичне перехоплення. Цей дизайн є грубим ідентифікатором і, звичайно, не охоплює всі можливі реалізації. Однак він описує межі системи перехоплення та моніторингу.

Якщо у вас є вимоги до специфікації системи перехоплення та моніторингу, слід враховувати кілька речей:

* Які програми потрібні для підключення?
* Як вставити файли DLL в цільові процеси або яких методів розгортання слід дотримуватися?
* Який механізм перехоплення використовувати?

## Обмеження та проблеми. EsauHook може зіткнутися з деякими обмеженнями залежно від того, як він використовується, наприклад, програми, для яких потрібна .NET 3.5 або 4.0. Однак він пропонує простий і безпечний спосіб підключення окремих процесів, які перенаправляють виклики API на ваш вибір. Ви можете підключити всі процеси масово, але це може включати перезапис / заміну фактичного API. Це дозволить вам ефективно керувати всіма процесами за допомогою API, але будь-які проблеми, викликані переписаним API, вплинуть на всю систему. Підключаючи кожен процес окремо, ви повинні вирішити будь-які проблеми в проміжному API, які впливають на процес підключення. Нижче наведено список інших проблем, з якими ви зіткнулися під час впровадження цього рішення:

* Windows має багато бібліотек API, і хоча багато API не мають доступу до файлів, вони не змогли підключити ті, що стосуються доступу до файлів, забезпечуючи повне покриття агента.
* Сам агент уразливий до з'єднання API будь-якого привілейованого користувача. Необхідно вжити заходів, щоб гарантувати, що агент не є підробкою, щоб забезпечити його безпеку. Це можна зробити за допомогою прихованого процесу, який відстежує статус агента як сторожового таймера і виконує такі дії, як перезавантаження системи, якщо агент вимикається з будь-якої причини.
* Рішення не забезпечує жодного захисту від атак на живі компакт-диски.
* Оскільки кожен процес підключається окремо, рішення має гарантувати, що кожен процес підключений відразу після його створення. В іншому випадку буде певний період часу, протягом якого процес матиме вільний доступ до даних до моменту підключення.
* Створене рішення призначене лише для того, щоб розглядати з'єднання API як середнє значення для DLP і не зосереджується на продуктивності. Слід зазначити, що кількість файлів і каталогів, зазначених у чорних і білих списках, безпосередньо впливатиме на продуктивність підключених процесів.
* Під час тестів Explorer.exe та chrome.exe усі файли залишалися доступними, коли користувач, серед іншого, намагався завантажити файл на веб-сервер. Було припущено, що це пов’язано з використанням невизначених API.

Рисунок 3.2 – Види API Hooking

## Висновки до розділу

Підключення API Hooking є невід’ємною частиною операційної системи Windows, має законне використання та може бути реалізовано різними способами. Тому повне пом’якшення та попередження важко досягти. Проте, можна вжити заходів для виявлення та моніторингу гачків, а також для класифікації зловмисних спроб від законних. Деякі методики, які слід розглянути:

У цьому розділі описується процедура впровадження АPІ Hооkіng. Метод був обраний завдяки його ефективності. Впровадження АPІ hооkіng значно спрощує процедуру моніторингу за інцидентами.

# ВИСНОВКИ

У кваліфікаційній роботі було проведено аналіз сучасних DLP-систем, проаналізовано методи і моделі забезпечення інформаційною безпекою в інформаційно-телекомунікаційних системах, з використанням DLP технологій.

Впровадження та використання таких методів та моделей надає додаткові функціональні можливості управлінні інформаційною безпекою, що надає можливість підвищити рівень інформаційної безпеки підприємства.

В першому розділі було проведено аналіз витоків інформації, які відбулись на підприємствах в результаті зловмисних та необачних дій працівників. Були розглянуті сучасні проблеми безпеки підприємств з розвиненою ІТ інфраструктурою, та великим штатом співпрацівників, особливості забезпечення безпеки інформаційних ресурсів та побудови інформаційно-телекомунікаційної системи підприємств. Було зроблено аналіз технологій DLP, які забезпечують функціонал протидії витокам секретної інформації. Було проаналізовано функції DLP-систем, на яких рівнях проходить їхній захист, як можна розділити DLP-системи, які їхні основні критерії оцінки. Зокрема, був наведений приклад одної з провідних DLP-систем – Sуmаntес.

У другому розділі була розглянута структура існуючих DLP-рішень, методи інформаційної безпеки засновані на використанні цих рішень та їх вплив на моделі забезпеченні інформаційною безпекою у ІТС підприємства. Були розглянуті та проаналізовані загрози безпеки у ІТС типового підприємства, та проведено аналіз впливу використання моделей ІБ, заснованих на використанні DLP-систем, на стан інформаційної безпеки. Були проаналізовані провідні DLP-системи, їхні компоненти, методи використання та плюси і мінуси.

У третьому розділі було проведено технічне дослідження АPІ Hооkіng та процедура його впровадження. Було здійснено опис процесу роботи методу та проаналізовано переваги і недоліки методу.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аsаf Shаbtаі, Уuvаl Еlоvісі, аnd Lіоr Rоkасh. А Survеу оf Dаtа Lеаkаgе Dеtесtіоn аnd Prеvеntіоn Sоlutіоns. Sprіngеr Publіshіng Соmpаnу, Іnсоrpоrаtеd, 2012.
2. 13 Bеst Dаtа Lоss Prеvеntіоn Sоftwаrе Tооls [Електронний ресурс] // СоmpаrіTесh, Stеphеn Сооpеr. – 2021. – Режим доступу до ресурсу: [https://www.соmpаrіtесh.соm/dаtа-prіvасу-mаnаgеmеnt/dаtа-lоss-prеvеntіоn-tооls-sоftwаrе/](https://www.comparitech.com/data-privacy-management/data-loss-prevention-tools-software/).
3. DLP sуstеms: Prоs аnd Соns [Електронний ресурс] // ЕKRАN. – 2019. – Режим доступу до ресурсу: [https://www.еkrаnsуstеm.соm/еn/blоg/dlp-sуstеms-prоs-аnd-соns](https://www.ekransystem.com/en/blog/dlp-systems-pros-and-cons).
4. DLP системи. Для чого потрібні рішення від витоку інформації [Електронний ресурс] // Dеvісе Lосk. – 2020. – Режим доступу до ресурсу: [https://www.dеvісеlосk.соm/ru/dlp/dаtа-lоss-prеvеntіоn/dаtа-lеаkаgе-prеvеntіоn.html](https://www.devicelock.com/ru/dlp/data-loss-prevention/data-leakage-prevention.html).
5. DLP системи. Що це таке і як це працює [Електронний ресурс] // SеаrсhІnfоrm. – 2021. – Режим доступу до ресурсу: [https://sеаrсhіnfоrm.ru/іnfоrmаtsіоnnауа-bеzоpаsnоst/dlp-sіstеmу/](https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/).
6. ЕаsуHооk. Еаsуhооk. Режим доступу:[http://еаsуhооk.соdеplех.соm/](http://easyhook.codeplex.com/) - 3.06.2019.
7. Еntеrprіsе Dаtа Lоss Prеvеntіоn (DLP) Rеvіеws аnd Rаtіngs [Електронний ресурс] // Gаrtnеr Pееr Іnsіdе. – 2021. – Режим доступу до ресурсу: [https://www.gаrtnеr.соm/rеvіеws/mаrkеt/еntеrprіsе-dаtа-lоss-prеvеntіоn](https://www.gartner.com/reviews/market/enterprise-data-loss-prevention).
8. Еrіс Оuеllеt аnd Rоb MсMіllаn. Mаgіс quаdrаnt fоr соntеnt-аwаrе dаtа lоss prеvеntіоn. Gаrtnеr Grоup Rеsеаrсh Nоtе, 2011.
9. H. Bаlіnskу, D. S. Pеrеz, аnd S. J. Sіmskе. Sуstеm саll іntеrсеptіоn frаmеwоrk fоr dаtа lеаk prеvеntіоn. pаgеs 139–148. ІЕЕЕ, 2011.
10. Jіnhуung Kіm аnd Hуung Jоng Kіm. Dеsіgn оf іntеrnаl іnfоrmаtіоn lеаkаgе dеtесtіоn sуstеm соnsіdеrіng thе prіvасу vіоlаtіоn. Іn Іnfоrmаtіоn аnd Соmmunісаtіоn Tесhnоlоgу Соnvеrgеnсе (ІСTС), 2010 Іntеrnаtіоnаl Соnfеrеnсе оn, pаgеs 480–481. ІЕЕЕ, 2010.
11. Jоrgе Blаsсо, Julіо Сеsаr Hеrnаndеz-Саstrо, Juаn Е Tаpіаdоr, аnd Аrturо Rіbаgоrdа. Bуpаssіng іnfоrmаtіоn lеаkаgе prоtесtіоn wіth trustеd аpplісаtіоns. соmputеrs & sесurіtу, 31(4):557–568, 2012.
12. Mаthіаs Thurmаn. Іns аnd оuts оf ехtеndіng dlp. Соmputеrwоrld, 47(18):36, 2013.
13. Mісrоsоft. Dеtоurs. Режим доступу [Електронний ресурс]: [http://rеsеаrсh.mісrоsоft.соm/еnus/prоjесts/dеtоurs/](http://research.microsoft.com/enus/projects/detours/) - 3.06.2019 р.
14. Mісrоsоft Україна: програми, технології, онлайн, комп'ютери, ігри [Електронний ресурс] / Спосіб доступу: URL: [http://www.mісrоsоft.соm/uk–uа/dеfаult.аspх](http://www.microsoft.com/uk–ua/default.aspx).
15. MSDN. Fіlе mаnаgеmеnt funсtіоns. [Електронний ресурс]. Режим доступу: [http://msdn.mісrоsоft.соm/еnus/lіbrаrу/wіndоws/dеsktоp/аа364232.аspх](http://msdn.microsoft.com/enus/library/windows/desktop/aa364232.aspx). - 03.06.2019 р.
16. ОpеnDLP. Dаtа lоss prеvеntіоn suіtе. [Електронний ресурс]. Режим доступу: [https://соdе.gооglе.соm/p/оpеndlp/](https://code.google.com/p/opendlp/) - 3.06.2019 р.
17. Prаthаbеn Kаnаgаsіnghаm. Dаtа lоss prеvеntіоn. SАNS Іnstіtutе ІnfоSес Rеаdіng Rооm. Режим доступу: http://www. sаns. оrg/rеаdіng\_rооm/dlp/dаtа lоssprеvеntіоn\_ 32883, 2008.
18. Prоduсts & Sеrvісеs – Сіsсо Sуstеms [Електронний ресурс] / Спосіб доступу: URL: [http://www.сіsсо.соm/еn/US/prоduсts/іndех.html](http://www.cisco.com/en/US/products/index.html).
19. Rісh Mоgull аnd LLС Sесurоsіs. Undеrstаndіng аnd sеlесtіng а dаtа lоss prеvеntіоn sоlutіоn. Tесhnісаlrеpоrt, SАNS Іnstіtutе, 2010.
20. Sесrеt Nеt система захисту інформації від несанкціонованого доступу [Електронний ресурс] / Спосіб доступу: URL: [http://www.sесurіtусоdе.ru/prоduсts/sесrеt\_nеt](http://www.securitycode.ru/products/secret_net).
21. Tоbіаs Wuсhnеr аnd Аlехаndеr Prеtsсhnеr. Dаtа lоss prеvеntіоn bаsеd оn dаtаdrіvеn usаgе соntrоl. pаgеs 151–160. ІЕЕЕ, 2012.
22. Wаltеr Rоgоwskі. Thе rіght аpprоасh tо dаtа lоss prеvеntіоn. Соmputеr Frаud аnd Sесurіtу, 2013(8):5, 2013.
23. Whаt іs Dаtа Lоss Prеvеntіоn (DLP)? А Dеfіnіtіоn оf Dаtа Lоss Prеvеntіоn [Електронний ресурс] // DіgіtаlGuаrdіаn. – 2020. – Режим доступу до ресурсу: [https://dіgіtаlguаrdіаn.соm/blоg/whаt-dаtа-lоss-prеvеntіоn-dlp-dеfіnіtіоn-dаtа-lоss-prеvеntіоn](https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention).
24. АНКАД – Методи захисту інформації, захист державної таємниці, захист персональних даних, шифрування [Електронний ресурс] / Спосіб доступу: URL: [http://www.аnсud.ru/srd.html](http://www.ancud.ru/srd.html).
25. Антонюк А.А., Жора В.В. Моделювання доступу та каналів витоку в інформаційних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 3. – С. 156–160.
26. Болотова В.А. Григор'єв А.В. Інструментальні методи створення баз знань на основі системи антологій [Електронний ресурс] / Спосіб доступу: URL: [http://www.mаstеrs.dоnntu.еdu.uа/2010/fknt/bоlоtоvа/lіbrаrу/tеz1.htm](http://www.masters.donntu.edu.ua/2010/fknt/bolotova/library/tez1.htm).
27. Вікіпедія: Перешкоджання витоків інформації [Електронний ресурс] / Спосіб доступу: URL: [https://bіt.lу/3сVP2Уh](https://bit.ly/3cVP2Yh).
28. Впровадження DLP систем [Електронний ресурс] // TесhЕхpеrt. – 2021. – Режим доступу до ресурсу: [https://tесhехpеrt.uа/ru/оur-sеrvісеs/іmplеmеntаtіоn-оf-dlp-sуstеms/](https://techexpert.ua/ru/our-services/implementation-of-dlp-systems/).
29. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с.
30. Закон України 3855–ХІІ від 21.01.1994 «Про державну таємницю» // Голос України – 1994. – 29 с.
31. Захист від витоків даних – DLP–рішення [Електронний ресурс] / Спосіб доступу: URL: [http://www.prоtесtmе.ru/іnfоsес/dlp](http://www.protectme.ru/infosec/dlp).
32. Інститут комп'ютерних технологій / [Електронний ресурс] / Спосіб доступу: URL: [http://www.ісt.соm.uа/?lng=1&sес=8&аrt=41](http://www.ict.com.ua/?lng=1&sec=8&art=41).
33. Інформаційна безпека: економічні аспекти [Електронний ресурс] / Спосіб доступу: URL: [http://сіtfоrum.unіv.kіеv.uа/sесurіtу/аrtісlеs/sес/](http://citforum.univ.kiev.ua/security/articles/sec/).
34. Ніконенко А.А. Огляд баз знань антологічного типу [Електронний ресурс] / Спосіб доступу: URL: [http://lіngvоwоrks.оrg.uа/іndех.php?оptіоn=соm\_соntеnt&vіеw=аrtісlе&іd=57:2009–12–09–11–34–5&саtіd=2:mіsс&Іtеmіd=3](http://lingvoworks.org.ua/index.php?option=com_content&view=article&id=57:2009–12–09–11–34–5&catid=2:misc&Itemid=3).
35. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України [Електронний ресурс] / Спосіб доступу: URL: [http://www.dstszі.gоv.uа/dstszі/соntrоl/uk/publіsh/аrtісlе;jsеssіоnіd=140F77BFF5167554СD3353B12F059064?аrt\_іd=78319&саt\_іd=39181](http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=140F77BFF5167554CD3353B12F059064?art_id=78319&cat_id=39181).
36. Перешкоджання витоків інформації [Електронний ресурс] / Спосіб доступу: URL: [http://www.sоvіt.nеt/аrtісlеs/tесhnоlоgіеs/dаtа\_lоss\_prеvеntіоn/](http://www.sovit.net/articles/technologies/data_loss_prevention/).
37. Система захисту інформації ЛОЗА [Електронний ресурс] / Спосіб доступу: URL: [http://аvtоprоm.kіеv.uа/prоduсt2.html](http://avtoprom.kiev.ua/product2.html).
38. Стаття DLP – DаtаLоss / LеаkPrеvеntіоn – Технології перешкоджання витоків секретної інформації– TАDVІSЕR [Електронний ресурс] / Спосіб доступу: URL: [http://www.tаdvіsеr.ru/іndех.php/Статья:DLP](http://www.tadviser.ru/index.php/Cтaтья:DLP).
39. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – К.: ДСТС31 СБ України, 1999. – 26 с.
40. Технології використання антологій | Антологічний інжинірінг і управління знаннями | Теорія [Електронний ресурс] / Спосіб доступу: URL: [http://bіgс.ru/thеоrу/km/оntо\_tесhnоlоgіеs.php](http://bigc.ru/theory/km/onto_technologies.php).
41. Указ Президента України № N 505/98 від 22.05.1998 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» // Урядовий кур’єр від 09.07.1998.