Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

_____ ***Сударикov Сергій Анатолійович***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.ф.-м.н., доц. Гусєв О.Ю.		
розділів:			
спеціальний	ст.викл. Святошенко В.О.		
економічний	к.е.н., доц. Волотковська Ю.О.		

Рецензент			

Нормоконтроль	к.ф.-м.н., доц. Гусєв О.Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

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

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

напряму підготовки (спеціальності) *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** (група) ***Сударикову Сергію Анатолійовичу*** (прізвище ім'я по-батькові)

Тема дипломної роботи ***Методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від _____ № _____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***система запобігання витоку інформації***

Предмет досліджень ***методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем***

Мета НДР ***підвищення рівня захищеності інформаційно-телекомунікаційних систем підприємства шляхом використання DLP технології***

Вихідні дані для проведення роботи ***існуючі алгоритми оцінки загроз інформаційної безпеки підприємства, результати досліджень компаній, InfoWatch, Symantec***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає у застосуванні сучасних методів та моделей забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології, що підвищує рівень захищеності підприємства***

Практична цінність ***полягає у зниженні часу на виявлення потенційних каналів витоку інформації за допомогою DLP системи***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Дати рекомендації щодо застосування запропонованої системи для типового підприємства

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Огляд джерел за темою та напрям досліджень	18.09.17-06.10.17
Методи досліджень	07.10.17-24.11.17
Результати досліджень	25.11.17-15.12.17
Виконання економічного розділу	16.12.17-29.12.17
Оформлення пояснювальної записки	30.12.17-10.01.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***економія досягається завдяки зниженню вірогідності витоку інформації при одноразових витратах на впровадження DLP системи***

Соціальний ефект ***застосування DLP системи підвищить рівень інформаційної безпеки підприємства***

7 ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Святошенко В.О.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Сударикова С.А.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.17р.
Термін подання дипломної роботи до ДЕК 16.01.18р.

РЕФЕРАТ

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

Об’єкт дослідження: система запобігання витоку інформації.

Предмет досліджень: методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем.

Мета роботи: підвищення рівня захищеності інформаційно-телекомунікаційних систем підприємства шляхом використання DLP технології.

В другому розділі було: проаналізовано існуючі на ринку DLP-систем. Було проведено аналіз ефективності методів та моделей забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем з використанням зазначених систем.

В економічному розділі розраховані капітальні та поточних витрати, величини збитків, загальний економічний ефект.

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

Розглянуті моделі управління інформаційною безпекою призначена для функціонування на підприємствах з метою попередження витоків ІзОД.

СИСТЕМА ЗАПОБІГАННЯ ВИТОКУ ДАННИХ, МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

РЕФЕРАТ

Пояснительная записка: __ с., _ рис., _ табл., _ приложения, источников.

Объект исследования: система предотвращения утечки информации.

Предмет исследований: методы и модели обеспечения информационной безопасности информационно-телекоммуникационных систем.

Цель работы: повышение уровня защищенности информационно-телекоммуникационных систем предприятия путем использования DLP технологии.

Во втором разделе было: проанализированы существующие на рынке DLP-систем. Был проведен анализ эффективности методов и моделей обеспечения информационной безопасности информационно-телекоммуникационных систем с использованием указанных систем.

В экономическом разделе рассчитаны капитальные и текущие расходы, величины убытков, общий экономический эффект.

Научная новизна работы заключается в разработке сведений о эффективности использования DLP систем.

Рассмотренные модели управления информационной безопасностью предназначены для использования на предприятиях с целью предотвращения утечек информации с ограниченным уровнем доступа.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ДАННЫХ, МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, МОДЕЛИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.

ABSTRACT

Explanatory note: __ pages, __ pictures, __ tables, __ additions, _ sources.

Object of research: information leakage prevention system.

Subject of research: methods and models of providing information security of information and telecommunication systems.

Purpose: to increase the level of protection of information and telecommunication systems of the enterprise by using DLP technology.

In the second section were analyzed existing on the market DLP-systems. An analysis of the effectiveness of methods and models of providing information security of information and telecommunication systems with the use of these systems was conducted.

In the economic section has calculated capital and operating costs, values of losses, total economic effect.

The scientific novelty of this work is a developing an information about effective use of DLP systems.

These models of information security management are intended for use in enterprises to prevent leakage of information with limited access.

DATA LOSS PREVENTION, MODELS OF INFORMATION SECUTITY MENEGMENT, METHODS OF INFORMATION SECUTITY MENEGMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

DLP – Data Loss/Leak Prevention, попередження витоку інформації;

АС – автоматизована система;

БД – база даних;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІР – інформаційні ресурси;

ІС – інформаційна система;

ІТ – інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

ЗІ – захист інформації;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПРД – правила розмежування доступу;

СЗІ – служба захисту інформації;

ТЗ – технічне завдання;

ТЗІ – технічний захист інформації.

ЗМІСТ

с.

ВСТУП

Рівень інформаційної безпеки є важливим критерієм ефективності функціонування для кожного підприємства. 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. Великий відсоток витоку здійснюється шляхом порушення політики безпеки, несанкціонованого доступу, навмисного та випадкового. Високий рівень інформаційної безпеки підприємства досягається шляхом розробки ефективної політики безпеки і, як наслідок, оптимальних правил розмежування доступу. Засоби, що реалізують політику безпеки, здійснюють контроль над взаємодією користувачів та інформаційних ресурсів, є ключовою частиною підсистеми керування доступом. Підвищення ефективності роботи цих засобів є важливим завданням.

Поширеність засобів захисту інформації (Gartner стверджує, що близько третини компаній вже використовують DLP) знімає тільки одну частину проблеми-випадкові витоку, – ніяк не впливають на зловмисні. Питання тут швидше в сприйнятті DLP-систем як програмного забезпечення, здатного самостійно, без зусиль з боку служб безпеки інформації, боротися з витоками, що в корені не вірно. І якщо з випадковими витоками DLP дійсно справляється, то боротьба зі зловмисними вимагає серйозної консалтингової складової в DLP-проектах на етапі підготовки впровадження та супроводу системи, розслідувань інцидентів.

Розпізнавання конфіденційної інформації в DLP-системах виробляється двома способами: аналізом формальних ознак (наприклад, гриф документа, спеціально введених міток, порівнянням хеш-функції) і аналізом контенту. Перший спосіб дозволяє уникнути помилкових спрацьовувань (помилок

першого роду), але зате вимагає попередньої класифікації документів, впровадження міток, збору сигнатур і т.д. Пропуски конфіденційної інформації (помилки другого роду) при цьому методі цілком вірогідні, якщо конфіденційний документ не піддався попередньої класифікації. Другий спосіб дає помилкові спрацьовування, зате дозволяє виявити пересилання конфіденційної інформації не тільки серед документів з грифом. У хороших DLP-системах обидва способи поєднуються.

Через цю тенденцію використання методів та моделей управління інформаційною безпекою в інформаційно-телекомунікаційних системах підприємства з використанням DLP-систем є актуальним питанням.

РОЗДІЛ 1. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ЦИРКУЛЮЮЧОЇ У ІТС ПІДПРИЄМСТВА

1.1 Стан питання

1.1.1 Актуальність обраної теми

2017 рік характеризується підвищенням витоку інформації, масовими кібератаками на інформаційні системи підприємств всіх форм власності. Одна із причин тенденції збільшення витоків – це збільшення частки держструктур і приватних підприємств які приділяють недостатню увагу до проблем захисту інформації. Друга причина – це масове використання мобільних пристроїв (смартфони, ноутбуки, планшети), до чого служби інформаційної безпеки державних і муніципальних організацій по країні виявилися явно не готові.

Поширеність засобів захисту інформації (Gartner стверджує, що близько третини компаній вже використовують DLP) знімає тільки одну частину проблеми-випадкові витоку, – ніяк не впливають на зловмисні. Питання тут швидше в сприйнятті DLP-систем як програмного забезпечення, здатного самостійно, без зусиль з боку служб безпеки інформації, боротися з витоками, що в корені не вірно.

І якщо з випадковими витоками DLP дійсно справляється, то боротьба зі зловмисними вимагає серйозної консалтингової складової в DLP-проектах на етапі підготовки впровадження та супроводу системи, розслідувань інцидентів.

1.1.2 Факти щодо витоку інформації за останні 5 років

За 2014 рік у світі зафіксовано і оприлюднено в ЗМІ понад 1200 випадки витоку конфіденційних даних, що на 19% перевищує показник минулих років.

Офіційно заявлені в ЗМІ збитки кредитно-фінансових організацій від витоків у першому півріччі 2015 року склали трохи більше 45,6 млн. доларів США.

Скомпрометовано більш 1,3 млрд записів, у тому числі фінансові та персональні дані.

Частка випадкових витоків стабільно зменшується і становить 39%.

Підвищується частка витоків у держкомпаніях і муніципальних установах – 27% (+ 9% порівняно з 2016 роком).

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

Самий популярний канал витоків – паперова документація 21,6%.

1.1.3 Статистика витоку інформації

У 2017 році Аналітичним Центром InfoWatch зареєстровано багато випадків витоку інформації з компаній приватного та державного сектору.

Скомпрометовані дані 31 млн користувачів віртуальної клавіатури.

Особиста інформація понад 31 млн користувачів інтелектуальної клавіатури A.I.type для Android-пристроїв витекла в Мережу. Розробники забули обмежити доступ до сервера, на якому розміщується база даних. Про це повідомляє портал ZDNet.

Сервер належить творцеві додатки A.I.type Ейтану Фітусі (Eitan Fitusi). Ресурс не був захищений паролем, що теоретично дозволяло будь-якому користувачеві Інтернету отримати доступ до великої бази даних об'ємом близько 577 ГБ. Проблему виявили дослідники безпеки з компанії Kromtech.

Відомо, що скомпрометована база включала основні дані користувачів: повне ім'я, місце розташування (країна і місто), адреса електронної пошти, а також час, що минув з моменту інсталяції програми. Найбільше не пощастило користувачам безкоштовної версії клавіатури – про них A.I.type збирала розширені відомості. Значна частина записів містили дані про використовувані пристроях на базі Android (модель телефону, IMEI, дозвіл екрана, версія ОС), IP-адреси і дані з Google-акаунтів (e-mail, дата народження, гендерна приналежність, фото профілю).

Крім того, фахівці Kromtech виявили кілька об'ємних таблиць з вельми чутливою інформацією з користувацьких пристроїв. В одній з них наведені 10,7 млн адрес електронної пошти, в інший – 374,6 млн телефонних номерів. У ряді інших файлів була інформація про завантажені додатки, в тому числі банківських. Природно, виникає цілком резонне питання – яким чином

розробники клавіатури звертался до цих даних і на якій підставі акумулювали їх у себе?

На сайті A.I.type відзначається, що «конфіденційність користувача є нашою головною турботою». Компанія-розробник запевняє, що будь-який текст, введений за допомогою віртуальної клавіатури, є зашифрованим. Однак, Kromtech знайшла докази того, що інформація подібного роду теж записується і зберігається.

Урядові веб-сайти скомпрометували дані жителів Індії.

Агентство Індії за унікальною ідентифікації (UIDAI) закрило 210 веб-сайтів державних відомств, котрі скомпрометували адреси, номери мобільних телефонів і інші персональні дані бенефіціарів кодів Aadhaar, повідомляє видання International Business Times.

Aadhaar є унікальним 12-значним номером і служить, крім іншого, посвідченням особи. З його допомогою громадяни Індії, особливо економічно слабкі верстви, можуть отримати доступ до урядових соціальних програм, наприклад, оформити субсидії. Індійський уряд прагне зробити Aadhaar ID обов'язковим, однак ця ініціатива зустрічає опір в суспільстві, особливо через побоювання громадян за збереження їх особистої інформації.

Як стало відомо, близько 210 сайтів місцевих та центральних органів влади, державних відомств і навчальних закладів, в спробі продемонструвати переваги володіння Aadhaar ID, розкрили особисті дані бенефіціарів. Скомпрометовані імена, адреси та інші персональні дані, вони були доступні необмеженому колу осіб невстановлений період часу.

На даний момент всі ці сайти заблоковані. UIDAI запевнило громадськість в тому, що буде проводити регулярні перевірки, щоб запобігти порушенням у майбутньому.

Скомпрометовані 1,7 млн акаунтів соціального сервісу IMGUR

Сервіс Imgur, один з найбільших ресурсів для зберігання та обміну фотографіями, зізнався в порушенні системи безпеки, що призвело до компрометації понад 1,7 млн користувальницьких акаунтів, передає BBC News.

Інцидент трапився ще в 2014 р, але більше трьох років в Imgur навіть не підозрювали про хакерську атаку. Витік був виявлений зовсім недавно – про неї компанію повідомив дослідник інформаційної безпеки Трой Хант (Troy Hunt).

На думку Ханта, реакція компанії на його повідомлення було зразковим. Протягом доби Imgur змогла оцінити масштаб інциденту, випустити офіційне повідомлення і почати скидання паролів на скомпрометованих записах. Представники сервісу зізналися, що викрадені паролі були зашифровані за допомогою застарілого алгоритму. Ніяких інших даних вкрадено не було, оскільки компанія не вимагає вказувати справжнє ім'я, адреса або номер телефону.

В даний час йде розслідування. Імовірно, алгоритм шифрування був зламаний хакерами методом «грубої сили». При цьому в Imgur відзначають, що в 2016 р впровадили більш досконалу систему шифрування.

Трой Хант зазначив, що близько 60% вкрадених адрес користувачів Imgur раніше вже містилися в базі «Have I Been Pwned?». До листопада 2017 року в ній налічувалося понад 4,8 млрд скомпрометованих акаунтів.

США звинуватили китайських хакерів у крадіжці комерційної таємниці SIEMENS, MOODY'S і TRIMBLE

Американська прокуратура пред'явила звинувачення трьом громадянам Китаю. Їм інкримінується участь в кібератаках на інформаційні системи німецького технологічного концерну Siemens, американського рейтингового агенства Moody's, а також американської компанії Trimble, що займається створенням систем геолокації. Інформація про це розміщена на сайті Міністерства юстиції США.

Відомо, що підсудні працювали в китайській компанії Boyusec (провінція Гуаньчжоу), яка надає послуги з інформаційної безпеки. За даними прокуратури, ця фірма була пов'язана з технологічно просунутої хакерської угрупованням Gothic Panda, тісно пов'язаної з китайськими спецслужбами.

У прокуратурі заявляють, що для злому комп'ютерних систем хакери використовували цільове фішингових шахрайство: в обрані компанії

відправляли листи з шкідливим вкладенням. Відкриття такого листа запускало програму викрадення комерційної інформації та інших даних.

В обвинувальних документах зазначається, що найбільшої шкоди дії хакерів завдали компанії Siemens. У 2015 р зловмисники викрали близько 407 ГБ даних з її підрозділів по транспорту, технологій і енергетики. Крім того, китайські кіберзлочинці зламали електронну пошту одного з економістів Moody's (можливо, вкрадена інформація аналітичного характеру може використовуватися для шантажу певних людей і компаній), а також атакували компанію Trimble, викравши не менше 275 МБ даних, що стосуються розробки нової навігаційної супутникової системи.

За даними джерела видання Forbes, жертвами Boyusec стали компанії, що представляють оборонну сферу, телекомунікації, транспорт і новітні технології. Також китайські хакери атакували урядові організації Гонконгу, США і ряду інших країн.

Нинішнє зростання пояснюється підвищеною увагою регуляторів, держави та інших зацікавлених сторін до проблеми безпеки даних. Через те що в іноземних державах кожен випадок витоку персональних даних громадян – привід для судового переслідування порушників, потерпілі та їхні адвокати охоче оприлюднюють всі випадки, пов’язані з порушенням встановлених процедур обробки і зберігання конфіденційної інформації з метою збільшити компенсаційні виплати. У результаті чого число витоків, які потрапили в ЗМІ, закономірно зростає. З іншого боку, регулюючі органи також активно поширюють інформацію про витік. Це характерно для США, де подробиці про витік даних періодично публікуються апаратом окружних прокурорів у вигляді повідомлень для преси.

Аналітики InfoWatch відзначали, що впровадження засобів захисту вплине на співвідношення випадкових і навмисних витоків. Наявні на ринку кошти і методи більш ефективні відносно саме випадкових витоків, ніж умисних. Як бачимо, відсоток випадкових витоків дійсно знижується – в 2015 частка випадкових витоків склала 43%. На цьому тлі зростає частка зловмисних

витоків – 42%. (Відсоток витоків неясною природи практично не змінився - 16% у 2016 р.).

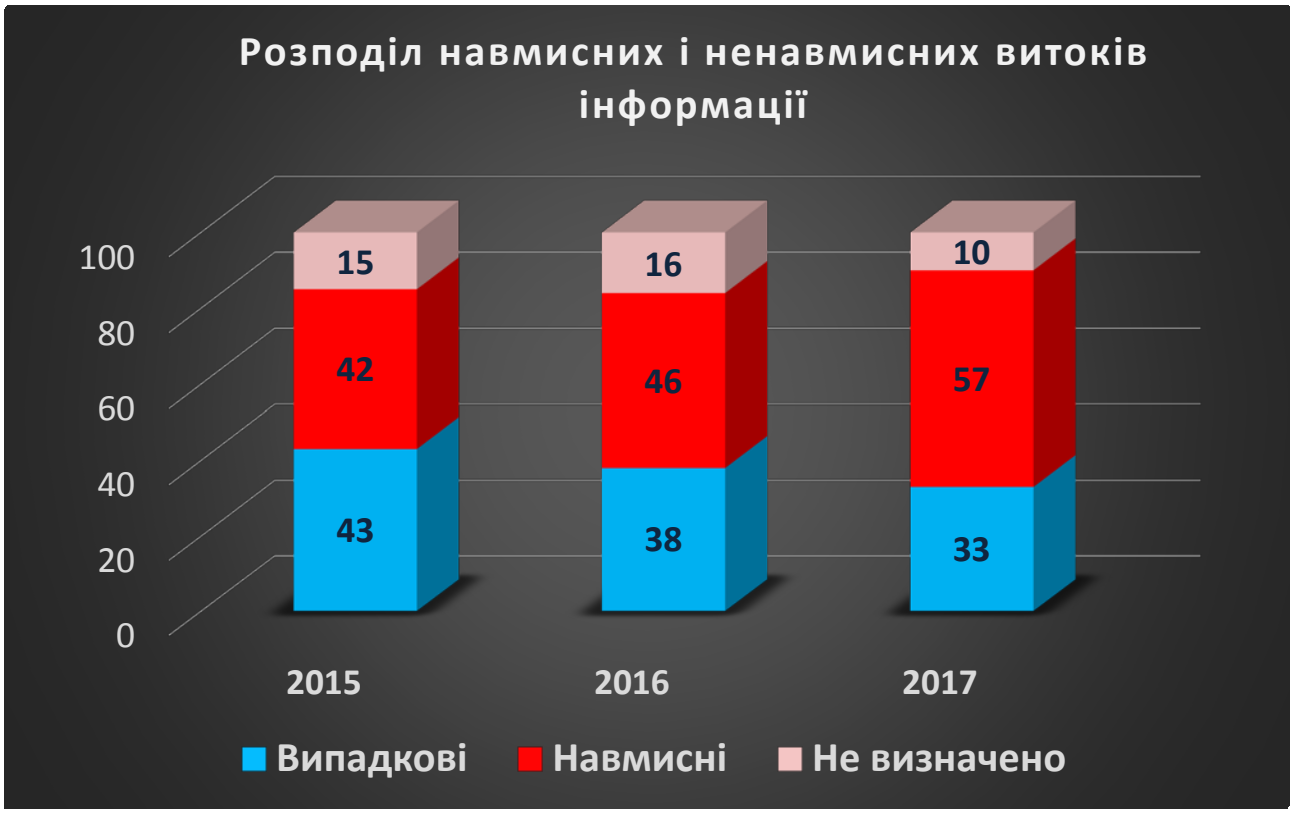
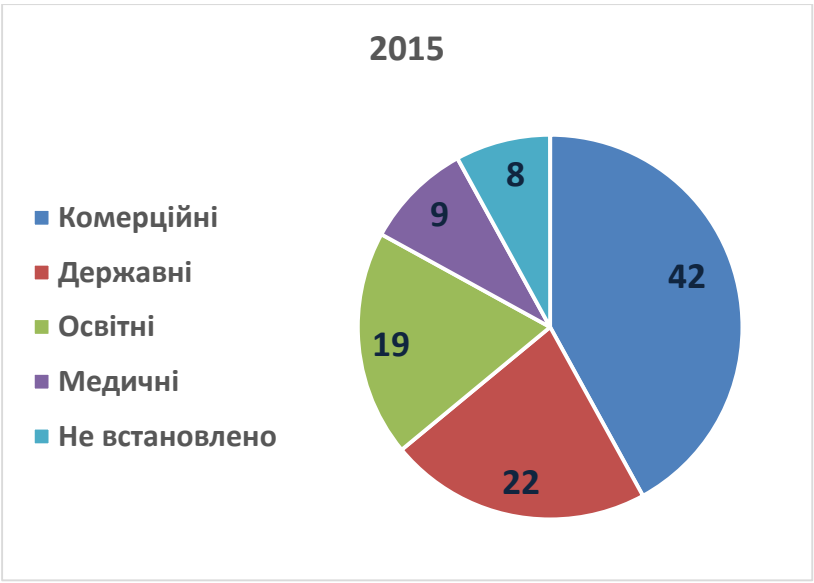


Рисунок 1.1 – Розподіл навмисних і ненавмисних витоків, 2015-2017рр.

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.



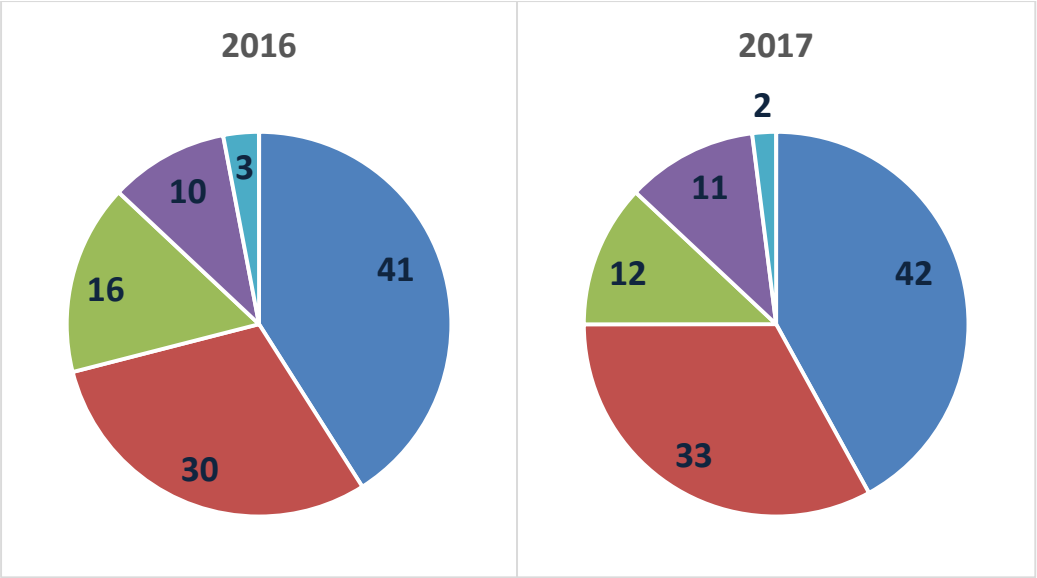


Рисунок 1.2 – Розподіл витоків інформації по організаціях, 2015-2017 рр.

Аналізуючи статистичні показники розподілу витоків за 2015-2017 років, можна відмітити зниження рівня витоків в освітніх організаціях до 12%, в порівнянні з 19% в 2015 році. Збільшення частки витоків комерційних та державних організацій пояснюється направленими діями у зв'язку веденням інформаційної війні між державами.

1.1.4 Статистика розподілу витоків за каналами

Канал витоків – характеристика, яка має пряме практичне застосування. Залежно від частоти та ймовірності витоків по тому або іншому каналу можна планувати впровадження засобів захисту, а також визначити пріоритет – якими каналами треба займатися в першу чергу. Але крім статистичних даних потрібно зважати на інформаційні потоки та методи передачі інформації та специфіку бізнес процесів.

На рисунку 1.3 зображено розподіл витоків по каналах.

Згідно отриманих результатів розподілу поширених каналів витоку, на першому місці знаходяться канали паперові носії, ПК, ноутбуки та смартфони. Витік інформації через паперові носії залишається актуальним та має значну вагу.

Одна із проблем запобігання витоків інформації із паперових документів це неможливість ефективно відслідкувати паперові носії.

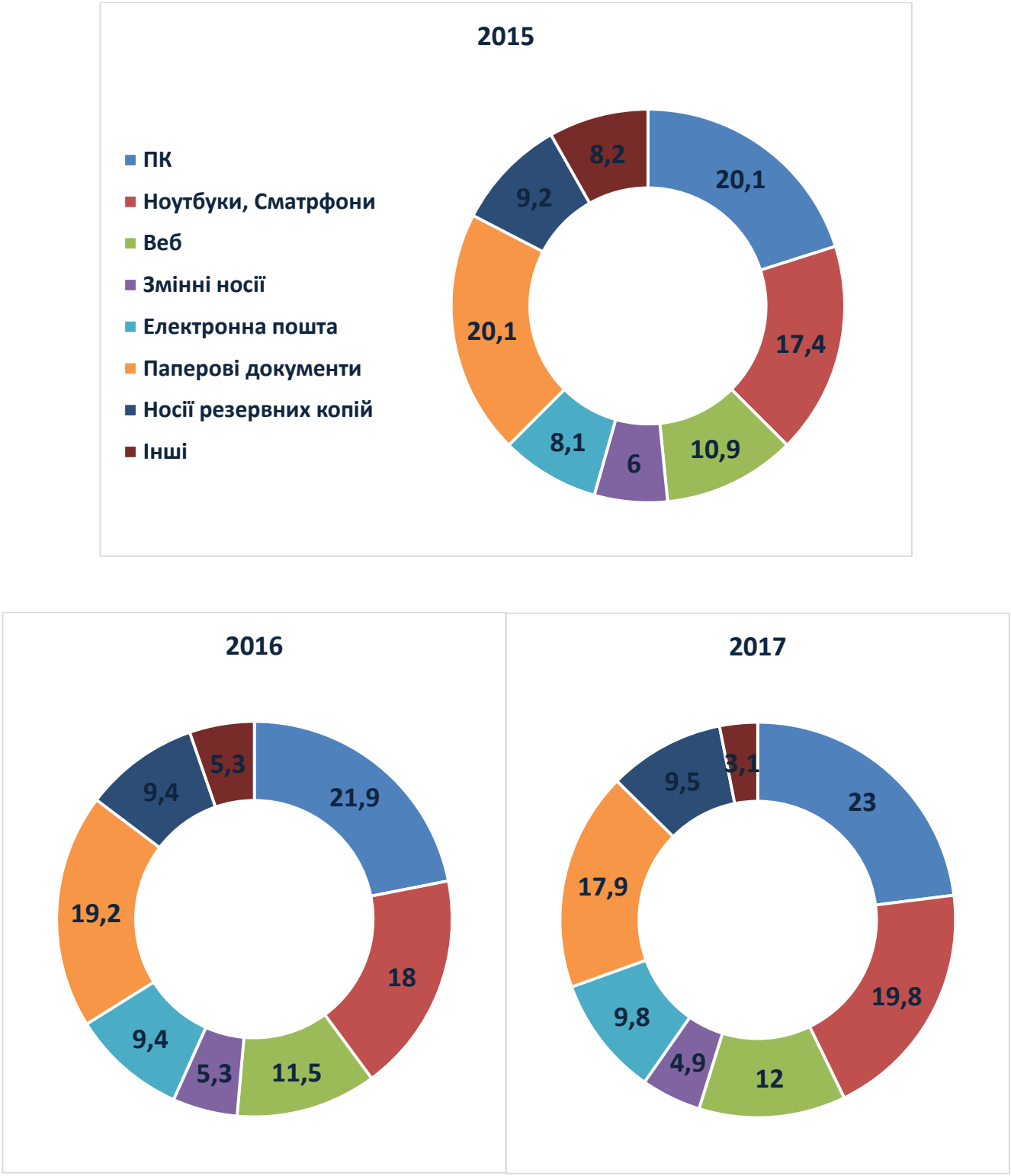


Рисунок 1.3 – Канали витоків інформації, 2016-2017рр.

Витоки із ПК займають велику частку, та зростають. Основними причинами витоків із ПК є поширення доступу до ПК між працівниками, використання неліцензійного програмного забезпечення.

Згідно докладу Borderless security: Ernst & Young’s 2015 Global Information

Security Survey,однієї з найбільших та авторитетних аудиторських компаній у світі Ernst & Young, 60% опитаних компаній відзначили підвищення рівня ризику у зв’язку з використанням соцмереж, cloud computing і портативних пристроїв. 64% опитаних відзначили розповсюдження важливих даних як один з топ-5 ризиків і 74% включили в топ-5 ризиків безперервний доступ критично важливих IT-ресурсів. У зв’язку з цим 50% досліджуваних компаній відзначили, що мають намір збільшити витрати на впровадження систем запобігання витоків інформації. Одному з ефективних заходів по запобіганню витоку даних є використання DLP-рішень (Data Loss/Leakage Prevention – запобігання втратам/витокам даних).

1.1.5 Забезпечення безпеки інформації циркулюючої у ІТС підприємства

Управління сучасним підприємством є складним комплексним завданням, що вимагає організації взаємодії ресурсів різного роду.

До таких ресурсів відносяться, зокрема, інформаційні системи, що забезпечують автоматизацію бізнес-процесів підприємства. Зазвичай до ІТ інфраструктури підприємства входять системи управлінням проектами, системи комунікації, бази даних, комп’ютерні мережі із серверами обробки та зберіганням даних та ін.

Тенденції бізнесу у сучасному світі зобов’язують підприємства до зберігання та обробляти велику кількості конфіденційної інформації, яка циркулює у ІТС та доступна до великої кількості працівників. Ґрунтуючись на бізнес потребах та службових зобов’язаннях працівників керівництво компаній часто надає працівникам доступ до великої кількості інформаційних ресурсів та засобів ІТС (електронна пошта, віддалене управління ПК, віддалений доступ до внутрішніх локальних мереж підприємства, внутрішні сервери обміну та зберігання даних).

Загрози інформаційній безпеці носять комплексний характер: зовнішні зловмисники здійснюють атаки на мережі і інформаційні ресурси організацій, а

власні співробітники, навмисно чи ні, часто стають джерелами конфіденційної інформації для третіх осіб. Зовнішні організації (конкуренти, преса, наглядові органи) і, нажаль, власні співробітники, що мають легальний доступ до оброблюваної інформації, зацікавлені в діставанні доступу до багатьох категорій оброблюваної інформації, зокрема до відомостей про клієнтів і історію роботи з ними, персональних даних співробітників, документів стратегічного розвитку, внутрішніх аналітичних звітів і багато чому іншому.

Стає очевидним що запобігання витокам інформації із ІТС підприємства стає одної з найважливіших завдань інформаційної безпеки, адже за статистикою 52,2% інцидентів витоку інформації трапляється у ІТС.

Використання традиційних на сьогодні заходів безпеки, таких як антивіруси і межмережеві фільтри виконують функції захисту інформаційних активів від зовнішніх загроз, але не яким чином не забезпечують захист інформаційних активів від витоку, спотворення або знищення внутрішнім зловмисником.

Велика кількість працівників які використовують у поведеній праці конфіденційну інформацію та об’єми комунікації й бізнес процесів ставить перед відділом ІБ важку задач контролю та запобігання витоком інформації у ІТС підприємства, через це останнім часом стає все більш поширеним використання DLP систем.

Згідно з наведеною статистикою частка випадкових витоків інформації у комерційних підприємствах знижується. Одна з причин цього феномену є упровадження DLP систем. З іншого боку доля навмисних витоків інформації все ще має тенденцію зростання. Це свідчить що DLP системи є більш ефективними при запобіганні випадкових витоків інформації, та при навмисних інтендантах порушники виявляються досить кваліфікованими що б викрасти вразливу інформацію.

Таким чином перед нами стає питання ефективності DLP систем як засобу ІБ підприємства. Саме навмисні витоки інформації складають більшу

потенційну загрозу, адже зловмисник має читку мету та плани що до використання викраденої інформації.

1.1.6 Інформаційно-телекомунікаційна система підприємства

Відповідно до статті 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле складають інформаційно-телекомунікаційна систему.

Компонентами інформаційної системи підприємства (виробництва) є банк даних і відповідні бази даних, використовувана мова (сукупність знаків і класифікаторів), а також комплекс моделей і програм, що забезпечують роботу з даними. Банк і бази даних являють собою сховище інформації та основний компонент інформаційної системи в багаторівневій інтегрованій автоматизованій системі управління підприємством.

Банк даних – комплекс, що охоплює спеціальні структури організації інформації, алгоритми, спеціальні мови, програмні й технічні засоби, що в сукупності забезпечують створення та експлуатацію системи накопичення інформації, яка надходить із декількох джерел, її оновлення, коригування та багатоаспектне використання в інтересах об’єктів управління підприємства, а також прямий зв’язок із користувачем для отримання відповіді на певні запити. Основні вимоги до банку даних: інтегрованість баз даних і цілісність кожної з них; незалежність; мінімальна збитковість даних, що зберігаються; здатність до розширення.

1.2 Аналіз технологій DLP

1.2.1 Загальні відомості о DLP системах

Data Leak/Loss/Leakage Prevention (DLP) – технології запобігання витоків конфіденційної інформації, що є власністю організації, за межі її інформаційної системи, а також комплекс технічних засобів (програмних або програмно-апаратних) для запобігання витокам.

DLP-системи будуються на аналізі потоків даних, що перетинають периметр захищається інформаційної системи. При виявленні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Як окремий програмний продукт DLP систему характеризуються наявністю наступного функціоналу: DLP-системи аналізують витікаючий трафік, DLP-системи проводять аналіз інформаційних потоків за декількома технологіями.

Також DLP-системи проводять глибокий аналіз змісту інформації та її катигорювання, організовує автоматичний захист конфіденційних даних в кінцевих інформаційних ресурсах, на рівні шлюзів передачі даних і в системах статичного зберігання даних, а також запускає процедури реагування на інциденти для вживання належних заходів.

Комплексні DLP системи зазвичай встановлюються на кінцевих пристроях – робочих станціях і серверах обробки даних, такі системи називаються мережевими, та призначаються для захисту корпоративної інформації від інсайдерських розкрадань. Також існують DLP-системи які встановлюються на рівні мережі та використовуються як шлюзове рішення, таки системи називаються хост-DLP.

1.2.2 Характеристика DLP-систем: Компоненти. Функції. Принцип роботи

На сьогоднішній день, DLP-системи є могутньою розподіленою інформаційною системою з єдиним центром управління, а також з низкою елементів, що забезпечують безпосереднє виконання прикладних функцій захисту інформації на контрольованих елементах інформаційної інфраструктури.

Залежно від архітектури побудови і умов функціонування сучасні DLP-системи можна поділити на наступні класи, які наведені в таблиці 1.1.

Таблиця 1.1 – Архітектура DLP-систем

Назва класу	Опис класу
Периметрові	Системи, що встановлюються в розрив каналу або одержуючи дзеркальну копію трафіку. Також до даного класу можна віднести системи, які інтегруються в компоненти інфраструктури (поштові сервери, web-сервери, сервера друку і т.д.) на рівні відповідних плагінів до них і забезпечують функціональність засобів захисту від витоків на мережевому рівні.
Агентські	Системи, агентські модулі яких встановлюються на робочі станції і несуть у собі базову функціональність захисту від витоків на рівні робочої станції.
Гібридні	Найбільш універсальні системи, які в своєму складі мають як периметрові так і агентські елементи.

Система DLP, як правило, складається з множини компонент. До складу типового рішення DLP, як правило, входять:

Центральний сервер управління, що виконує наступні функції:

- об’єднання решти компонентів рішення в єдину систему;
- визначення даних, що містять конфіденційну інформацію;
- створення, редагування і розповсюдження політик роботи з конфіденційними даними;
- збір, зберігання і обробку інцидентів, створення і розсилку звітів;
- надання ролевого доступу до управління системою співробітникам служби інформаційній безпеці.

Модулі моніторингу і блокування конфіденційної інформації, що передається по мережевих каналах. Вони можуть бути представлені як одним пристроєм, що реалізовує обидві функції, так і окремими (наприклад, Network Monitor, Network Prevent for Web, Network Prevent for E-mail).

Скануючий модуль – це додатковий компонент, який допоможе визначити місцезнаходження конфіденційної інформації в мереж підприємства. За допомогою цього модуля виконується сканування робочих станцій співробітників, файлових серверів, баз даних і так далі. Після завершення

процесу виводиться детальний звіт по кожному комп'ютеру або каталогу із загальним доступом. Крім того, якщо створити відповідну політику, такий модуль зможе переміщувати знайдену конфіденційну інформацію з робочих станцій співробітників, каталогів із загальним доступом і інших ресурсів в місце, задане адміністратором. Наприклад, це може спеціальний файловий сервер, де повинна зберігатися подібна інформація. Тобто, даний модуль не тільки оптимізує роботу адміністратора, але і упорядковує зберігання даних на серверах компанії.

Мережевий модуль аналізує повний обсяг вихідного трафіку підприємства. Саме завдяки цьому компоненту співробітники відділу IT-безпеки можуть контролювати, яка інформація «витікає» за межі корпоративної мережі. Поза сумнівом, що такі Web-сервіси як корпоративна пошта, електронна пошта з Web-доступом і системи миттєвих повідомлень є основним каналом для передачі «секретів». Мережевий модуль виконує не тільки аудит витоків конфіденційної інформації, але і здатний заблокувати подібні спроби.

Агенти для робочих станцій і серверів, що забезпечують контроль:

– переміщення конфіденційних даних на змінні носії інформації (USB, CD/DVD і ін.);

– переміщення даних до буферу обміну (функція «Вставка/Копіювання»);

– функції зняття знімка з екрану («Print Screen»);

Агенти також виконують функцію пошуку конфіденційних даних на локальних дисках.

Агент на робочій станції контролює дії, які співробітник виконує з конфіденційною інформацією. Кожен агент DLP-рішення оснащений своїм функціоналом, проте є базовий набір функцій, який властивий всім рішенням:

– блокування або аудит на запис для USB-пристроїв;

– блокування або аудит на запис CD/DVD-дисків;

– блокування або аудит на переміщення конфіденційних документів на файлові сервери;

– блокування або аудит при друкуванні матеріалу на локальному або мережевому принтері.

Основні функції DLP системи:

Перша – це ідентифікація, тобто виявлення конфіденційної інформації і місць її зберігання в мережі компанії. Крім цього система може здійснювати аналіз легітимності зберігання виявленої інформації в її поточному місцезнаходженні і при необхідності здійснювати перенесення в захищені сховища.

Друга функція – це моніторинг, в рамках якого система відстежує дані, що передаються і виявляє порушення відповідно до умов, заданих в політиках.

Третя функція – це захист. Дана функція може бути представлена різними діями. Це може бути і розсилка сповіщень про порушення політик безпеки, і ізоляція в карантин, і блокування передачі даних.

Захист конфіденційної інформації здійснюється DLP-системою за допомогою використання наступних основних функцій:

– Фільтрація трафіку по всіх каналах передачі даних;

– Глибокий аналіз трафіку на рівні контента і контексту.

– Захист конфіденційної інформації в DLP-системі здійснюється на трьох рівнях: Data-in-Motion, Data-at-Rest, Data-in-Use.

Data-in-Motion – дані, які передаються по мережевих каналах:

– Web (HTTP/HTTPS протоколи);

– Інтернет–меседжери (ICQ, QIP, Skype, MSN, WhatsUpp, Telegram, і так далі);

– Корпоративна і особиста пошта (POP, SMTP, IMAP і так далі);

– Безпровідні системи (WiFi, Bluetooth, 3G і так далі);

– FTP – з’єднання.

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

– Серверах;

– Робочих станціях;

– Ноутбуках;

– Системах зберігання даних (СЗД).

Data-in-Use – дані, які використовуються на робочих станціях.

Заходи, направлені на запобігання витоків інформації складаються з двох основних частин: організаційних і технічних.

Захист конфіденційної інформації включає організаційні заходи по пошуку і класифікації наявних в компанії даних. В процесі класифікації дані розділяються на 4 категорії:

– Таємна інформація;
– Конфіденційна інформація;
– Інформація для службового користування;
– Загальнодоступна інформація.

На другому етапі, після виконання організаційних методів, відбувається впровадження технічних засобів, які контролюють доступ до даним і здійснюють моніторинг ЛОМ компанії, запобігаючи витоку.[4]

Ефективна система протидії витокам повинна включати проактивну компоненту (DLP), реактивну компоненту (архів подій) і функціонал, що дозволяє реалізувати вибірковий контроль в режимі реального часу .

Проактивна компонента системи забезпечує аналіз потоків даних і запобігання/фіксацію факту передачі конфіденційній інформації.

Реактивна компоненту системи забезпечує реєстрацію і архівацію подій по основних каналах витоку даних (пошта, Інтернет, зовнішні носії, вивід на друк), а також надає функціонал для вибіркового контролю дій співробітників і розслідування інцидентів.

Функція контролю дій співробітників в режимі реального часу дозволяє організувати цільовий моніторинг і оперативне реагування на спроби "винесення".

Функції управління системою (завдання правил реагування, політик, логіки класифікації інформації) повинні виконуватися з єдиної консолі і передбачати гнучкий розподіл прав доступу. Принаймні, частина названих

функцій реалізована в самих різних продуктах: їх поставляють виробники засобів шифрування, захисту клієнтських систем, між мережевих екранів.

З точки зору технології система DLP повинна реалізовувати порівняння шаблонів ключових слів, точне порівняння даних, карантин для файлів при порушенні ними політики безпеки, передбачати можливість задавати комбінації даних для порівняння і виявлення при зберіганні і при переміщенні, а також включати засоби виведення звітів.[6]

Класифікація DLP-систем

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

Пасивні DLP-системи – це розслідування інцидентів, що відбулися. Дані системи не уміють блокувати витік інформації, але здатні надати вичерпні відомості про джерело і канали витоку.

Цей тип систем почав розвиватися як відповідь на потребу першого підходу до інформаційної безпеки, при якому знайти порушників важливіше, ніж запобігти витоку конфіденційної інформації. Такі системи складаються з перехоплювачів сніфферів, що копіюють всі електронні повідомлення, які відправляються по основних каналах комунікації: корпоративною і Web-поштою, соціальним мережам, IM, FTP, принтерам і USB-носіям.

Копії повідомлень зберігаються в архіві. Перед архівацією електронного повідомлення система перевіряє його на відповідність політиці ІБ компанії і у разі невідповідності політиці автоматично сповіщає офіцера безпеки.

Активні DLP-системи – це блокування витоку конфіденційної інформації в режимі реального часу.

Зазначені системи дозволяють контролювати переміщення конфіденційної інформації по всіх основних каналах комунікації: усередині ЛОМ (наприклад, між віддаленими підрозділами), через Інтернет (корпоративна і Web-пошта, соціальні мережі, WhatsUpp, Vider, FTP і т.д.), а також на з’ємні носії, принтери і тощо. В залежності від налаштованих політик

такі системи можуть працювати в режимі як блокування, так і моніторингу. Такі системи прийшли до нас з-за кордону, де дуже добре працює законодавство, що оберігає таємницю приватного життя. Тому у таких систем, як правило, відсутній повноцінний архів (зберігаються не всі електронні повідомлення, а тільки ті, які порушили політику безпеки компанії), і не можна відновити все листування співробітників при розслідуванні.

Для навчання рядових користувачів роботі з конфіденційними даними у деяких виробників активних DLP-систем закладена можливість повідомлення відправника з проханням підтвердити відправку документа. В цьому випадку співробітник усвідомлює, що вся відповідальність за пересилку конфіденційної інформації буде покладена на нього.

Потреба в комбінованих DLP-системах виникає при одночасній необхідності архівації всіх електронних повідомлень для подальшого розслідування і можливості блокування витоку конфіденційних даних через основні канали комунікацій. Такі системи починають з’являтися на ринку, але реалізують бажаний «повний комбінований» функціонал тільки частково. На сьогоднішній день отримати повноцінну комбіновану DLP-систему можна шляхом інтеграції декількох продуктів.

1.2.3 Технології ідентифікації і аналізу конфіденційних даних в DLP-системах

В DLP-системах зазвичай використовуються три методи ідентифікації: імовірнісний, детерміністський і комбінований. Системи, засновані на першому методі, здебільшого використовують лінгвістичний аналіз контента і «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацьовувань. Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм не вистачає гнучкості. Комбінований підхід поєднує обидва методи з аудитом середовища зберігання і обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації.

В системах DLP застосовуються складні механізми аналізу: порівняння по шаблонах з використанням словників і регулярних виразів, лінгвістичний і контекстний аналіз, цифрові відбитки. Словники і шаблони зручно застосовувати в конкретних областях, наприклад, для контролю номерів кредитних карт і інших персональних даних [2, 6].

У лінгвістичному і контекстному аналізі використовуються морфологія і статистичні моделі, враховується контекст, характер відправника і одержувача інформації. Цей метод хороший для динамічних даних. Цифрові відбитки (аналогічні сигнатурам в антивірусних продуктах) підходять для контролю статичних даних, наприклад, для захисту інтелектуальної власності.

Через DLP-систему проходять всі інформаційні потоки підприємства, і система повинна визначати, чи відноситься інформація, що передається до тієї, що захищається. Для цього використовують наступні технології:

– Сигнатури – пошук в потоці даних "заборонених" слів, послідовності символів ("стоп-слів");

– Лінгвістичні методи – працюють із словоформами, аналізують весь текст (наприклад, визначення частоти зустрічальності термінів);

– Цифрові відбитки – хеш-функції зразків конфіденційних документів;

– Регулярні вирази – дозволяють знаходити збіги за формою даних (а не за самими даними), типу номерів кредитних карток;

– Мітки – установка на файли, що містять конфіденційну інформацію, спеціальних «міток»;

– Штучний інтелект – самонавчальний алгоритм аналізу даних "Vector Machine Learning".

Методом аналізу є пошук в потоці даних деякої послідовності символів («стоп-слів»). У переважній більшості випадків сигнатурні системи налаштовані на пошук декількох слів і частоту зустрічальності термінів.

Метод аналізу масок є розширенням функціонала пошуку сигнатур і є пошуком такого змісту, який неможливо точно вказати в базі "стоп-слів", але можна вказати його елемент або структуру. До такої інформації слід віднести

будь-які коди, які характеризують персону або підприємство: ІНН, номери рахунків документів і так далі. Шукати їх за допомогою сигнатур неможливо.[17]

Лінгвістичний аналіз і база контентної фільтрації

Лінгвістичний метод аналізу тексту несе на собі характеристику всього класу методів аналізу вмісту. З погляду класифікації хеш-аналіз, аналіз сигнатур, аналіз масок – є "контентною фільтрацією", тобто фільтрацією трафіку на основі аналізу вмісту.

Технологія лінгвістичного аналізу дозволяє автоматично визначати тематику і ступінь конфіденційності аналізованого фрагмента інформації на підставі термінів, що зустрічаються в ньому, і їх поєднань. Лінгвістичний аналіз виконується на основі заздалегідь створеної бази контентної фільтрації (БКФ).

База контентної фільтрації – це база даних, яка представляє собою виділений на основі імовірнісних і математичних методів ієрархічно організований список (дерево) категорій з довільною кількістю вкладених рівнів, і що містить слова і вирази, наявність яких в документі дозволяє визначити тематику і ступінь конфіденційності інформації.

БКФ не тільки описує категорії інформації, яка циркулює в компанії, але і враховує різні атрибути її конфіденційності, в т.ч. специфіку діяльності компанії, її вимоги до безпеки.

Результатами проведення лінгвістичного аналізу тексту автоматично привласнюються ті або інші категорії, відповідні його тематиці і змісту. У аналізованій інформації можуть зустрітися терміни (слова і словосполучення) з різних категорій, тому вона може бути віднесена до однієї або декількох категорій БКФ.

База контентної фільтрації і точність детектування конфіденційної інформації

Надійність і точність ідентифікації конфіденційних даних в корпоративних інформаційних потоках за допомогою технології лінгвістичного

аналізу залежать від бази контентної фільтрації, на основі якої здійснюється аналіз.

Тому важливо створити базу, яка забезпечить надійні результати фільтрації інформації за категоріями. Основним методом лінгвістичного аналізу за допомогою БКФ є пошук в аналізованому фрагменті інформації слів і словосполучень, що описують конфіденційні дані і структурованих за категоріями.

1.2.4 Створення бази контентної фільтрації

Для створення БКФ спочатку потрібно скласти її структуру – рубрикатор або дерево контентних категорій. Таким деревом є ієрархічний список з категоріями і підкатегоріями.

Потім кожну категорію потрібно наповнити списком термінів, ключових слів, словосполучень і фраз, поява яких в аналізованому фрагменті інформації вказує на його приналежність до певної контентної категорії.

Після цього для кожного терміну / словосполучення встановлюється вага, яку цей термін матиме при віднесенні інформації до певної категорії. Рішення про те, чи є текст релевантним контентній категорії, приймається за наслідками порівняння загальної суми ваги термінів, знайдених в тексті, з порогом релевантності цієї категорії. Для забезпечення якісної категоризації базу контентної фільтрації необхідно підтримувати в актуальному стані – редагувати категорії, що змінюються з часом, додавати і/або видаляти терміни і словосполучення, змінювати їх вагу і ін.

1.2.5 Технології цифрових відбитків

Найбільш перспективні технології, при яких проводяться певні математичні перетворення початкового файлу (алгоритми перетворень виробниками не розкриваються). Процес перетворення будується таким чином: початковий файл – математична модель файлу – цифровий відбиток. Такий процес дозволяє істотно скоротити об’єм оброблюваної інформації (об’єм цифрового відбитку не більше 0,01 від об’єму файлу). Цифрові відбитки потім

розміщуються в центральному репозитарії (Oracle, MS SQL) і можуть бути продубльовані в оперативній пам’яті пристрою, що здійснює аналіз інформації (залежить від вендора і типу розгортання). Відбитки потім використовуються для порівняння і аналізу інформації, що передається. При цьому відбитки файлу, що передається, і «модельного» файлу можуть співпадати не обов’язково на 100%, відсоток збігу може задаватися. Технології стійкі до редагування файлів і застосовні для захисту практично будь-яких типів файлів: текстових, графічних, аудіо, відео. Кількість «помилкових спрацьовувань» не перевищує одиниць відсотків (всі інші технології дають 20-30% помилкових спрацьовувань). Ця технологія стійка до різних текстових кодувань і мов, які використовуються в тексті.

1.2.6 Регулярні вирази

Регулярні вирази – система синтаксичного розбору текстових фрагментів за формалізованим шаблоном, заснована на системі запису зразків для пошуку. Наприклад, номера кредитних карт, телефонів, адреси e-mail, номери паспорта, ліцензійні ключі.

1.2.7 Статистичні методи

Статистичні технології відносяться до текстів не як до зв’язної послідовності слів, а як до довільної послідовності символів, тому однаково добре працюють з текстами на будь-яких мовах. Оскільки будь-який цифровий об’єкт – хоч картинка, хоч програма представляє собою послідовність символів, то вищезазначені методи можуть застосовуватися для аналізу не тільки текстової інформації, але і будь-яких цифрових об’єктів.[8]

1.2.8 Контейнерний аналіз («рішення на мітках»)

Метод аналізує властивості файлу або іншого контейнера (архіву, криптодиска і тому подібне), в якому знаходиться інформація. Просторічна назва таких методів – «рішення на мітках», що досить повно відображає їх суть. Кожен контейнер містить якусь мітку, яка однозначно визначає тип контейнера контенту, що міститься усередині. Згадані методи практично не вимагають

обчислювальних ресурсів для аналізу переміщуваної інформації, оскільки мітка повністю описує права користувача на переміщення контенту по будь-якому маршруту. У спрощеному вигляді такий алгоритм звучить так: «є мітка – забороняємо, немає мітки – пропускаємо».

1.2.9 Самонавчальний алгоритм аналізу даних Vector Machine Learning

Технологія аналізу і запобігання витокам даних, заснована на принципах штучного інтелекту і здатна самостійно ідентифікувати дані, доступ до яких повинен бути обмежений. В ході ряду незалежних тестів вона показала вражаючі результати.

VML покликана подолати обмеження існуючих технологій ідентифікації документів. Використовуючи зразки наявних даних, програмне рішення на базі алгоритмів VML можна навчити дізнаватися ключові характеристики і визначати внутрішні відмінності конфіденційних і неконфіденційних даних. Такий підхід усуває необхідність створення правил, заснованих на ключових словах, і застосування "цифрових відбитків" до всіх нових документів при їх створенні.

1.2.10 Критерії оцінки DLP-систем як програмного продукту

Компанія Forrester Research склала основні чотири критерії оцінки DLP-систем.

Перший критерій – багатоканальність. DLP-система бути комплексною та охоплювати максимальну кількість каналів витоку інформації: e-mail, Web і IM, а також моніторинг файлових операцій та потоків в ІТС.

Другий критерій – уніфікований менеджмент. Система повинна володіти уніфікованими засобами управління всіх компонентів, які входять до її складу. Головна вимога це здійснення управління всіма частинами системи із одного місця.

Третій критерій – активний захист. Система повинна не тільки фіксувати витоки конфіденційної інформації, але і ефективно їх блокувати у разі необхідності.

Четвертий критерій – класифікація інформації за вмістом та контентом, категорювання інформації. Методи, які використовуються для забезпечення контролю витоків конфіденційної інформації повинні враховувати наступні складові: тип протоколу, вид операції, ідентифікацію користувача і т.д.

Згідно до цих критеріїв можна зробити висновок що майже сучасні DLP системи є об’ємними та комплексними програмними продуктами. Вибір DLP повинен основуватись згідно із технічних та програмних технологіях використовуваємих на підприємстві, та відповідати потребам ІБ що до каналів витоку інформації у компонентах ІТС.

1.2.11 Компоненти DLP системи

Розглянемо склад DLP системи на прикладі програмного рішення Symantec Data Loss Prevention (РСДРП). Продукт SDLP забезпечують захист для широкого спектру типів конфіденційних даних, що знаходяться в мережах і системах зберігання даних, а також на комп’ютерах співробітників незалежно від того, працюють вони в мережі підприємства або поза нею.

1.3 Symantec Data Loss Prevention Enforce Platform

Центральним компонентом для продукту є платформа управління Symantec Data Loss Prevention Platform, яка дозволяє визначати і поширювати на інші компоненти рішення політики щодо запобігання втрати конфіденційних даних. Даний компонент також надає єдиний веб-інтерфейс для управління і роботи з рішеннями лінійки SDLP.

1.3.1 Symantec Data Loss Prevention Network Discover

Компонент Symantec Data Loss Prevention Network Discover виявляє незахищені конфіденційні дані, скануючи такі інформаційні ресурси, як файлові сховища, бази даних, поштові сервери, веб-сервери і т.п.

1.3.2 Symantec Data Loss Prevention Data Insight

Компонент Symantec Data Data Loss Prevention Insight дозволяє відстежувати доступ до конфіденційної інформації для автоматичного

визначення власників цих даних, що дозволяє підвищити гнучкість процесів виявлення конфіденційних даних і управління ними.

1.3.3 Symantec Data Loss Prevention Network Protect

Компонент Symantec Data Loss Prevention Network Protect є доповненням, розширюють функціональність компонента Symantec Data Loss Prevention Network Discover в частині зниження ризику втрати незахищених конфіденційних даних шляхом перенесення цих даних з публічних сховищ на мережевих серверах в карантин або захищені сховища.

Компоненти SDLP мережі Discover і SDLP Захист мережі здійснюють захист від втрати конфіденційних даних зі наступних інформаційних ресурсів:

- мережеві файлові системи (CIFS, NFS, DFS та ін);
- локальні файлові системи на робочих станціях і ноутбуках;
- локальні файлові системи (Windows, Linux, AIX, Solaris);
- БД Lotus Notes;
- Microsoft Exchange;
- Microsoft SharePoint;
- Documentum та ін.

1.3.4 Symantec Data Loss Prevention Endpoint Discover і Symantec Data Loss Prevention Endpoint Prevent

Ці компоненти представлені двома модулями:

Агент SDLP Agent, який встановлюється на робочі станції користувачів (у тому числі ноутбуки) і забезпечує виконання таких функцій:

- виявлення незахищених конфіденційних даних на користувача робочих станціях;

- блокування передачі конфіденційних даних (змінні носії інформації, CD / DVD, друк, засоби обміну миттєвими повідомленнями і т.п.).

Сервер SDLP Endpoint сервер, який забезпечує зв’язок агентів SLDP Агент з платформою управління SDLP Enforce Platform і дозволяє визначати

політики моніторингу конфіденційних даних і блокування їх передачі з користувача робочих станцій.

Агент SDLP Agent запобігає витоку конфіденційних даних з користувацьких робочих станцій і корпоративних ноутбуків при спробі їх передачі з використанням:

– зовнішніх накопичувачів інформації (USB, SD, Compact Flash, FireWire);

– запису на CD/DVD;

– мережі (HTTP / HTTPS, електронна пошта / SMTP, FTP, IM);

– коштів друку / факсу;

– копіювання конфіденційних даних в буфер обміну.

1.3.5 Symantec Data Loss Prevention Network Monitor

Компонент Symantec Data Loss Prevention Network Monitor в реальному часі відстежує мережевий трафік на наявність конфіденційної інформації і формує повідомлення при спробі передачі такої інформації за межі внутрішньої мережі.

1.3.6 Symantec Data Loss Prevention Network Prevent

Компонент Symantec Data Loss Prevention Network Prevent блокує передачу конфіденційної інформації засобами поштових і веб-комунікацій.

Компоненти SDLP Network Monitor і SDLP Network Prevent забезпечують захист від витоків конфіденційних даних при спробі їх передачі такими способами:

- електронна пошта (SMTP);
- засобу обміну миттєвими повідомленнями (IM);
- веб-пошта, форуми, соц. мережі і т.д. (HTTP, HTTPS);
- протокол передачі файлів (FTP);
- торренти;
- Telnet;
- будь-які інші сесії через будь-який порт TCP.

1.4 Постановка задачі

В другому розділі дипломної роботи буде проведено аналіз методів та моделей забезпечення інформаційною безпекою у інформаційно-комунікаційних системах на DLP технології.

1.5 Висновок

В даному розділу було проведено аналіз витоків інформації, які відбулись на підприємствах в результаті зловмисних та необачних дій працівників. Динаміка витоків інформації за останні 5 років свідчить об актуальності систем запобігання витоків, адже спостерігається постійне зростання кількості витоків інформації. Розглядаючи статистику за останні 3 роки виникає питання ефективності DLP систем.

Були розглянуті сучасні проблеми безпеки підприємств з розвиненою IT інфраструктурою, та великим штатом співпрацівників, особливості забезпечення безпеки інформаційних ресурсів та побудови інформаційно-телекомунікаційної системи підприємства.

Зроблено аналіз технологій DLP, які забезпечують функціонал протидії витокам конфіденційної інформації і можуть бути впровадженні до складу КЗЗ, з метою мінімізації ризиків фінансових та репутаційних збитків.

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

2.1 Огляд систем попередження витоку інформації (DLP)

2.1.1 Загальні відомості

Запобігання витоків (англ. Data Leak Prevention, DLP) – технології запобігання витоків конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витоків.

DLP-система – це програмний продукт, який дозволяє виявити і блокувати несанкціоновану передачу конфіденційної інформації (її витік) з якого-небудь електронним каналом комунікації, використовуючи інформаційну інфраструктуру підприємства.

Технічно контрольованими DLP-продуктом каналами можуть виступати:

- електронна пошта;
- веб-ресурси – публічні поштові сервіси, соціальні мережі, форуми, блоги, чати тощо;
- програми для обміну миттєвими повідомленнями (WhatsUpp, Skype і т.п.).
- зовнішні пристрої, підключені до робочих станцій або серверів (USB-диски, CD/DVD, локальні принтери, несанкціоновані передавачі WiFi, Bluetooth, модеми тощо).

DLP-система повинна забезпечити можливість виявити випадкове або навмисне несанкціоноване використання інформації співробітниками компанії, а не перекривати повністю всі канали. Крім того, на думку експертів, найважливіший критерій зарахування рішення до класу DLP - це наявність можливостей автоматичного або ручного аналізу подій, що відбулися і переданої інформації (у режимі реального часу або т.зв. пост-аналізу архіву накопиченої інформації). За-

хідними колегами з аналітичних агентств для класифікації DLP-рішень часто використовується критерії комплексності захисту (охоплення різних каналів) і можливості блокування витоку конфіденційних даних (активні політики інформаційної безпеки). DLP-система дає можливість комплексного підходу до захисту від витоків інформації та мінімізації їх наслідків: можуть бути проаналізовані такі події як відправка конфіденційного документа на принтер, електронну пошту, флеш-накопичувач, пересилання частини конфіденційного документа за допомогою IM-агента і т.д. Крім цього, за допомогою сучасних DLP-систем можна отримати багато "корисною" інформації про своїх співробітників.

Сучасне DLP-рішення дозволяє здійснювати перехоплення мережевого трафіку і, на підставі бази алгоритмів і сигнатур, відновлювати передані повідомлення. У повідомленнях присутній вся доступна метаінформація (одержувач, відправник, тема, інші заголовки) і передані файли. Наприклад, DLP-система від компанії SearchInform, дозволяє перехоплювати дані безпосередньо на робочих місцях, в тому числі і на використовуваних в організації ноутбуках і нетбуках, незалежно від того, перебувають вони в корпоративній мережі чи ні. Система збирає відправлені дані і передає їх для аналізу відділу ІБ, як тільки ноутбуки знову опиняється в корпоративній мережі.

2.1.2 Критерії вибору DLP системи: обсяг і структура даних

Обсяг даних впливає на вибір типу DLP і сценарію роботи. Відмінності мережевих, змішаних і хостових DLP будуть детально розглянуті в главі масштабованість, а на сценарії роботи хотілося б зупинитися докладніше. Зазвичай при впровадженні DLP постає питання вибору між активним і пасивним режимом роботи. У першому випадку DLP ставиться "в розрив" всіх проходять через кордони мережі даних і активно блокує недозволену передачу інформації, у другому система працює строго в повідомному режимі, тобто не блокує передачу, а лише повідомляє про підозрілі інциденти, заносячи всю інформацію про кожного в журнал подій.

Існує і змішаний режим, коли DLP ставиться "в розрив", але політики налаштовуються таким чином, що запобігають тільки самі явні порушення, а інший

трафік пропускається без будь-якої модифікації. Крім того, в активному режимі у більшості систем є можливість ручної перевірки, тобто підозрілі дані поміщаються в "карантин" і очікують ручної перевірки співробітником безпеки. Сценарій впровадження впливає на сукупну вартість володіння – у довгостроковій перспективі пасивний режим вимагає великих трудовитрат на аналіз трафіку і розслідування, у той час як в активному режимі DLP автоматично блокує більшу частину витоків. При цьому вимоги до обладнання для всіх сценаріїв приблизно однакові – як мінімум один продуктивний сервер, хоча при невеликому навантаженні можна встановити DLP прямо на проксі-, поштову або будь-який інший діючий сервер.

Структура та перелік даних, що захищаються в першу чергу впливають на набір технологій виявлення витоків, яким повинна володіти DLP-система. Загальний перелік можливих технологій включає в себе сигнатурний і лінгвістичний аналіз, пошук по базах регулярних виразів і "цифрових відбитків", OCR (виявлення тексту на пересилаються зображеннях) і самонавчальні технології. На жаль, поки що далеко не кожна DLP-система пропонує хоча б половину з наведених технологій.

Кожна технологія оптимальна лише для певного типу даних. «Цифрові відбитки» - одна з найбільш популярних і простих у застосуванні технологій, проте вона ефективна для виявлення досить об'ємних документів, рідко піддаються змінам. "Регулярні вирази" ідеальні для виявлення передачі персональних даних та інформації з типовою структурою – номерів рахунків, телефонів, адрес і т.д. Лінгвістичні технології (морфологія) добре працюють з більшістю типів даних, проте їх ефективність залежить від старанності налаштування, яку, як правило, можуть забезпечити лише професійні лінгвісти.

2.1.3 Критерії оцінки DLP системи: контрольовані канали комунікацій

Повноцінні DLP-системи також повинні контролювати і інші канали комунікацій. В першу чергу сюди відноситься Інтернет-трафік: Інтернет-пейджери, веб-пошта, соціальні мережі, блоги, форуми, файлообмінники, FTP, пірингові мережі, сервіси відправки SMS і т. д.

Далеко не всі рішення вміють контролювати весь перелік потенційних каналів витоку. Так, у більшої частини західних DLP-рішень контроль популярних у Україні та СНД каналів комунікацій поки викликає серйозні проблеми. Наприклад, передані через інтернет-messenger дані можуть аналізувати лише кілька DLP-рішень на ринку.

2.1.4 Критерії оцінки DLP системи: необхідність розслідування інцидентів

Розслідування інцидентів – важлива частина будь-якої системи захисту від витоків даних. Найчастіше на практиці необхідно не тільки виявляти і блокувати витоку, а й проводити службове розслідування по кожному інциденту. Таке розслідування може включати в себе як аналіз безпосередньо виявлених конфіденційних даних, так і ретроспективний аналіз активності користувача або групи користувачів. На жаль, багато DLP не тільки не дозволяють довільно архівувати перехоплювали дані, але і не зберігають заблоковану інформацію. У такому випадку неможливо зрозуміти, що насправді було заблоковано, адже навіть сама технологічна DLP-система може помилитися.

2.1.5 Критерії оцінки DLP системи: захист даних при зберіганні

Останнім часом втрату конфіденційних даних все частіше відносять до DLP, і багато провідні рішення вже давно оснащуються системами криптографічного захисту. На перший погляд ймовірність втрати важливих даних здається куди меншою, ніж, наприклад, ймовірність копіювання конфіденційних файлів на USB-накопичувач, однак все більше витоків відбувається саме внаслідок втрати магнітних стрічок, флешок і ноутбуків. Деякі DLP-рішення мають вбудований функціонал для надійного захисту даних при зберіганні за допомогою сучасних алгоритмів шифрування – AES, AES-XTS

2.1.6 Критерії оцінки DLP системи: масштабованість

Як і будь-яке IT-рішення, будь-яка DLP-система спочатку орієнтована на певний розмір мережі і обсяг трафіку. Кожен продукт розрахований на певний розмір мережі, обсяг і структуру даних, які йому необхідно аналізувати. Хоча

деякі DLP позиціонуються на великі організації з більш ніж 500 робочими станціями, їх застосування майже завжди переважно і для середніх компаній з парком від 100 до 500 комп'ютерів.

Формально можна розділити на хостової DLP, що встановлюються на кінцеві точки мережі – настільні комп'ютери і ноутбуки, мережеві та змішані. Чисто хостової DLP, т. е. контролюючі на рівні агентів як зовнішні пристрої та принтери, так і всі мережеві канали витоку, останнім часом набувають все більшого поширення. Їх безперечні переваги – простота і відносна дешевизна, проте хостової DLP мають ряд істотних недоліків: низькі продуктивність, масштабованість, відмовостійкість, високі вартість подальшої підтримки та вимоги до характеристик кінцевих точок мережі. Практика показує, що безболісно використовувати такі DLP можна лише в невеликих організаціях.

Подібних недоліків позбавлені мережеві DLP, вони переносять основне навантаження - мережевий трафік і його архівування – в єдину точку, яку можна досить легко масштабувати, а саме рішення інтегрувати з існуючими продуктами – проксі-серверами, меж мережевими екранами і антивірусами. При цьому суто мережеві DLP для захисту від витоків через кінцеві точки мережі вимагають застосування сторонніх продуктів для контролю зовнішніх пристроїв та мережевих принтерів, однак майже всі лідируючі рішення мають свої полегшені агенти. Такі агенти на відміну від суто хостових DLP практично не навантажують робочі станції та ноутбуки і часто мають куди більш великий функціонал, ніж розраховані на малі мережі продукти "все в одному". Комбінація продуктивність і масштабованість мережевого DLP і полегшених агентів є оптимальною для середніх і великих організацій.

2.1.7 Порівняння існуючих DLP рішень

2.1.7.1 Програмне рішення на базі ПЗ виробника SecurIT

Zecurion Zgate – програмне забезпечення для контролю мережевого трафіку для запобігання витоків (крадіжки, втрати, випадкової пересилання) конфі-

денційної інформації. Zgate відноситься до сімейства IPC / DLP-систем і дозволяє контролювати SMTP-, HTTP-, HTTPS-, FTP-і інший інтернет-трафік. Для пошуку і блокування передачі конфіденційних даних у Zgate використовуються різні технології детектування: сигнатури, лінгвістичний аналіз, регулярні вирази, метод Байєса, «цифрові відбитки» і власні.

Zecurion Zlock – програмне забезпечення для захисту від витоків конфіденційної інформації шляхом розмежування прав доступу користувачів до зовнішніх і внутрішніх пристроїв комп'ютера і до локальних і мережевих принтерів. Zecurion Zlock відноситься до сімейства IPC / DLP-систем і дозволяє архівувати роздруковуються на принтері документи і файли, що записуються на USB-, CD-, DVD-носії та інші пристрої.

2.1.7.2 Програмне рішення на базі ПЗ виробника SearchInform

КІБ (Контур Інформаційної Безпеки) має модульну архітектуру, дозволяючи підключати лише необхідні користувачу компоненти. Робота КІБ реалізована на двох платформах:

EndpointSniffer – трафік перехоплюється спеціально вбудованими агентськими модулями на рівні робочих станцій користувачів;

NetworkSniffer – трафік перехоплюється на рівні мережевих комутаторів.

В обох випадках перехоплення даних здійснюється непомітно для користувача, блокування одержуваних і даних, що відправляються не відбувається. КІБ здійснює контроль і протоколювання (включаючи тіньове копіювання) доступу користувачів до периферійних пристроїв, портів вводу-виводу і мережевим протоколам. Для КІБ реалізована інтеграція з доменною структурою Windows, яка дозволяє:

– визначити, під обліковим записом якого користувача і з якого комп'ютера відправляється зовні конфіденційна інформація;

– тимчасово або постійно виключити з моніторингу того чи іншого доменного користувача;

– розмежувати права доступу співробітників служби безпеки підприємства так, щоб кожен з них мав доступ до певної частини перехопленої інформації в межах своєї компетенції.

2.1.7.3 Програмне рішення на базі ПЗ виробника FalconGaze

SecureTower – програмне рішення, розроблене компанією Falcongaze, створене спеціально для захисту корпоративної інформації від витоків, а також для контролю активності співробітників на робочих місцях.

SecureTower контролює популярні канали корпоративної комунікації, і дозволяє в ретроспективі відстежувати інциденти, пов'язані з порушенням політик інформаційної безпеки компанії. Передбачена можливість створення гнучких правил безпеки, відповідних потребам організації. Вся перехоплена інформація піддається аналізу за змістом, за атрибутами, і за допомогою статистичних даних. Мається функціонал, що дозволяє здійснювати контроль інформації безпосередньо з баз даних без додаткових операцій з вивантаження інформації з БД. Систему можна використовувати в будь-якої корпоративної мережі незалежно від її розмірів і топології. Система може бути використана в територіально-розподілених офісах компаній, що мають віддалені філії та представництва.

Система контролює ноутбуки та нетбуки, що залишають межі компанії. Вся передана інформація з мобільної робочої станції перехоплюється і фіксується в повному обсязі і передається службі безпеки компанії при підключенні портативного пристрою до корпоративної мережі. В системі містяться інструменти, що дозволяють аналізувати діяльність співробітників на робочих місцях.

Таблиця 2.1 – Порівняння технічних можливостей DLP систем

Виробник	**SecurIT**	**SearchInform**	**FalconGaze**
Названа системи	ZGate	КІБ	SecureTower
Модульність системи	+	+	-
Місто встановлення	На сервер + ZLock на клієнтський ПК	Сервер, клієнт	Сервер, клієнт
Ліцензування	Почтові ящики, робочі місця	Сервер, mail, IM, Skype, Print, device, HTTP, FTP	Робоче місце

Продовження таблиці 2.1

Виробник	**SecurIT**	**SearchInform**	**FalconGaze**
Ролі	Деяка кількість	Деяка кількість	Адміністратор безпеки, офіцер безпеки
Контроль IM	+	+	+
Контроль HTTP/HTTPS, FTP	+	+	+
Контроль Skype	+	+	+
Контроль E-mail	+	+	+
Соціальні мережі і блоги	+	+	+
Контроль зовнішніх пристроїв	При покупці Zlock	+	-
Контроль портів	USB, COM, LPT, Wi-Fi, Bluetooth	USB, LPT	USB, LPT
Блокуємі протоколи	HTTP, HTTPS, SMTP, OSCAR, IM	SMTP, POP3, MAPI, IMAP, HTTP,FTP, IM	HTTP, HTTPS, FTP, FTTPS, Вся пошта и IM
Аналіз за словником	+	+	+
Лінгвістичний аналіз	+	+	+
Аналіз трансліту	+	n/a	n/a
Аналіз архівів	+	+	+
Аналіз малюнків	+	+	-
Стандартні шаблони фільтрації	+	+	+
Затримка відправки підозрілих повідомлень	+, ОБ приймає рішення	n/a	Ні, тільки інформування офіцера ИБ
Логування дій адміністраторів системи	+	n/a	У разі установки агенту на ПК адміністратора
Режим установки агентів	Відкритий	n/a	Таємний/Відкритий
Захист агентів від вимикання	+	+	+
Запис звітів в локальне сховище	+	+	+

Продовження таблиці 2.1

Виробник	**SecurIT**	**SearchInform**	**FalconGaze**
Перегляд історії інцидентів	+	+	+
Режими сповіщень	Консоль, пошта, графіки	Консоль, пошта, графіки	Консоль, пошта, графіки

2.1.7.4 Можливі методи забезпеченні ІБ засновані на використанні DLP систем

Будуючись на технічних характеристиках DLP-систем, можливі наступні методи забезпеченні ІБ.

Таблиця 2.2 – Методи ІБ із використанням DLP-систем

	Метод ІБ	**Приклади реалізації**
1	Фільтрація витікаючої інформації по ключовим словам, регулярним виразам для ідентифікації конфіденційних даних	Системи фільтрації трафіку
2	Установка грифів конфіденційності на документи, що захищаються, в електронному вигляді і стеження за його життєвим циклом	Системи мандатного доступу до документів і протоколювання звернень
3	Стеження за маніпуляціями з конфіденційними даними і протоколювання дій користувача на робочому місці	Системи контролю дій користувача
4	Управління доступом до пристроїв введення-виводу	Системи контролю знімних носіїв
5	Сканування даних, що зберігаються на робочих місцях з метою виявлення по зліпках конфіденційних відомостей	Системи сканування сховищ і робочих станцій
6	Виконання всього комплексу вищезазначених підходів і зведення управління політиками і подіями до єдиної консолі	Комплексна DLP-системи
7	Аналіз протоколів різноманітних систем безпеки в уніфікованому вигляді і виявлення аномальних активностей з боку співробітників і зовнішніх зловмисників	Системи Computer Forensics (netForensics та інші)

Продовження таблиці 2.2

Метод ІБ		Приклади реалізації
8	Контроль доступу користувачів до комп'ютерів і інформаційних систем з додатковими елементами контролю	Системи двохфакторної аутентифікації системи з використанням біометрії
9	Розгалужена система розмежування прав доступу до конфіденційних документів	Системи класу Enterprise Rights Management (Microsoft RMS) і захищеного документообігу
10	Шифрування носіїв конфіденційної інформації	Системи шифрування сховищ, дисків накопичувачів

2.1.7.5 Аналіз змін у моделях забезпеченні ІБ з використанням DLP систем

На основі порівнянь технічних властивостей оглянутих DLP систем була розроблена таблиця впливу систем запобігання витоку інформації на моделі забезпеченні інформаційної безпеки. Результати зображенні у таблиці 2.3

Таблиця 2.3 – Вплив DLP систем на моделі УІБ

Виробник	**SecurIT**	**Search Inform**	**FalconGaze**
Названа системи	ZGate	КІБ	SecureTower
Розділення персоналу за ролями	+	+	+
Контроль веб протоколів	+	+	+
Автоматичне блокування підозрілих повідомлень	+	+	-
Контроль зовнішніх пристроїв	+	+	-
Контроль зовнішніх портів	+	+	+
Реєстрування виявлених інтендантів порушення безпеки	+	+	+
Реєстрування дій адміністратора системи	+	-	+/-
Контроль дій користувачів	+	+	+
Аналіз та фіксування порушень безпеки серед користувачів	+	+	+

2.1.7.6 Висновки щодо впливу використання DLP-систем на моделі інформаційної безпеки у ІТС

Базуючись на функціональних можливостей DLP-систем, та можливих методах забезпеченні ІБ з використанням цих систем, слідую що використання DLP-систем несе наступні позитивні зміни до функціональних можливостей моделі управління:

– фільтрація витікаючої інформації по ключовим словам, регулярним виразам для ідентифікації конфіденційних даних;

– установка грифів конфіденційності на документи, що захищаються, в електронному вигляді і стеження за його життєвим циклом;

– стеження за маніпуляціями з конфіденційними даними і протоколювання дій користувача на робочому місці;

– управління доступом до пристроїв введення-виводу;

– сканування даних, що зберігаються на робочих місцях з метою виявлення по зліпках конфіденційних відомостей;

– управління політикамиі подіями до єдиної консолі;

– аналіз протоколів різноманітних систем безпеки в уніфікованому вигляді і виявлення аномальних активностей з боку співробітників і зовнішніх зловмисників;

– контроль доступу користувачів до комп'ютерів і інформаційних систем з додатковими елементами контролю;

– розгалужена система розмежування прав доступу до конфіденційних документів.

2.2 Аналіз інформаційної безпеки ІТС

2.2.1 Інформаційна безпека ІТС

Інформаційна безпека передбачає забезпечення захисту інформації та інфраструктури, що здійснює її підтримку, від будь-якого випадкового або ж зловмисного втручання, в результаті якого інформація може бути втрачена, нанесені збитки її безпосереднім власникам та інфраструктурі, що підтримує її зберігання

й існування. Інформаційна безпека виконує завдання, пов’язані з прогнозуванням і запобіганням можливим подібним діям, а також зводить до мінімуму можливий збиток.

Стан інформаційної безпеки підприємства являє собою уміння і здатність підприємства протистояти будь-яким спробам завдати шкоди його законним інтересам.

Задачами системи інформаційної безпеки є:

– віднесення інформації до категорії обмеженого доступу

– протидія витоку такої інформації;

– прогнозування, своєчасне виявлення й усунення загроз інформаційній безпеці підприємства; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню нормального функціонування і розвитку;

– створення механізму й умов оперативного реагування на загрози інформаційній безпеці;

– ефективне припинення посягань на інформаційні ресурси підприємства на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки.

Об’єктами безпеки є:

– інформація про персонал (керівництво, співробітники);

– інформація щодо технологій, які використовуються;

– інформація о клієнтах;

– інформація о проектах;

– інформаційні ресурси (інформація з обмеженим доступом, що складає комерційну таємницю, інша конфіденційна інформація, надана у виді документів і масивів незалежно від форми і виду їхнього представлення)

2.2.2 Структурна інформаційна безпека підприємства

Структурно інформаційну безпеку підприємства складають: безпека інфо-

рмаційних ресурсів, безпека інформаційної інфраструктури та безпека "інформаційного поля" підприємства.

Підприємство займається самостійно формуванням інформаційних ресурсів, використовуючи засоби обчислювальної техніки і зв'язку, які забезпечують обробку, зберігання і передачу інформації.

Безпека ІТС полягає у такому стані захищеності електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку підприємства яка забезпечує цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює).

Основними задачами забезпечення безпеки інформаційних ресурсів є:

– запобігання витоку інформації о клієнтах;

– запобігання витоку інформації о проектах;

– організація та контроль доступу співпрацівників до необхідних інформаційних ресурсів, відповідно із виробничою необхідністю або посаді (топ менеджери та менеджери відповідних департаментів);

Найбільш суттєвими загрозами безпеки інформаційних ресурсів є витік або втрата таких ресурсів (зокрема інформація о клієнтах та проектах).

Основними загрозами інформаційній безпеці підприємства є:

– несприятливі події природного, техногенного і соціального характеру;

– збої, відмови, руйнування/пошкодження програмних і технічних засобів;

– терористи і кримінальні елементи;

– залежність від постачальників / провайдерів / партнерів / клієнтів;

– працівники, які реалізовують загрози ІБ з використанням легально наданих їм прав і повноважень (внутрішні порушники ІБ);

– працівники, що реалізовують загрози ІБ без легально наданих їм прав і повноважень, а також суб'єкти, що не являються працівниками підприємства.

Основними організаційно-технічними заходами щодо забезпечення інформаційної безпеки є:

– постійний і всебічний аналіз інформаційної системи з метою виявлення уразливості інформаційних активів підприємства;

– своєчасне виявлення проблем, потенційно здатних вплинути на інформаційну безпеку підприємства, корегування моделей загроз і порушника;

– розробка і впровадження заходів захисту, відповідно до аналізу ризиків ІБ, та актуального стану КСЗІ;

– контроль ефективності впроваджених заходів захисту;

– персоніфікація та розподіл ролей і відповідальності між співробітниками;

– проводити аудит ІБ із урахування порушень безпеки, ризиків та загроз ІБ;

– планові перевірки ризиків, використовуючи інформацію о технологічних організаційних змін у бізнесі та інформаційній безпеці підприємства;

– вести запис дій та подій які можуть мати вплив на ефективність ІБ підприємства;

– вносити зміни до планів безпеки з метою забезпечення упровадження результатів діяльності по контролю та моніторингу системи.

2.3 Структура інформаційно-телекомунікаційної системи типового підприємства

ІТС підприємства що забезпечує її діяльність та виконання всіх бізнес процесів та задач можна представити у вигляді ієрархії наступних основних рівнів:

– фізичного (лінії зв'язку, апаратні засоби та ін.);

– мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

– мережевих додаткових програм |мережних| і сервісів;

– операційних систем ;

– систем управління базами даних.

Основні функціональні елементі ІТС є наступні елементі ІС:

– робочі станції;

– сервери (файлів, баз даних, служб друку і т. п.);

– мережеві пристрої (маршрутизатори, комутатори, шлюзи і т. п.);

– засоби зв'язку і передачі даних;

– засоби захисту інформації;

– канали і лінії зв'язку.[6]

Основу інформаційної системи складає база даних первинних документів, також до неї входять сервери обробки та зберігання даних із серверами додатків які реалізують таки компоненти ІТС як системи електронної пошти, системи керування та ведення проектів, системи контролю версій, бази знань.

Загальна схема ІТС типового підприємства зображена на рисунку 2.1

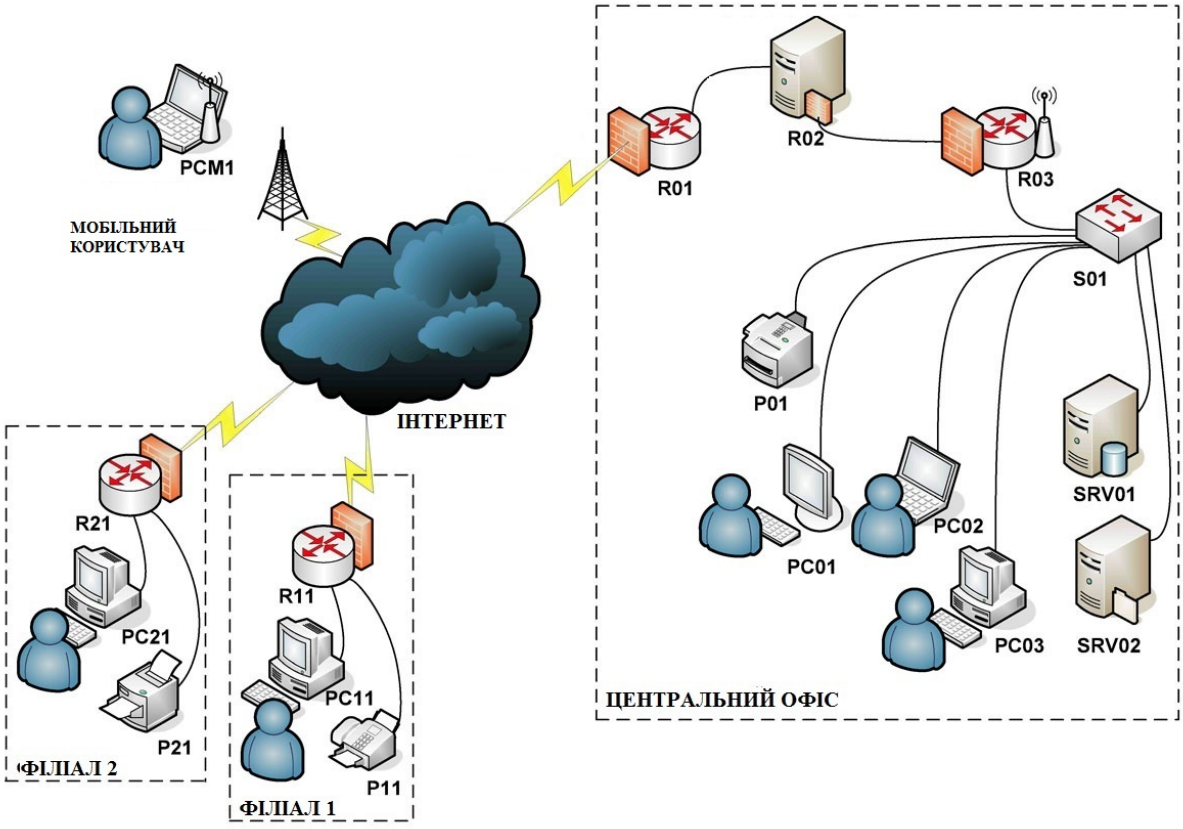


Рисунок 2.1 - Загальна схема ІТС типового підприємства

2.4 Аналіз інформації циркулюючої на типовому підприємстві

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

Таблиця 2.4 – Інформація циркулююча на підприємстві

Інформація	**Режим доступу**	**Правовий режим**	**Співробітник, маючий доступ**
Проектна документація	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітники безпосередня працюючі над проектом
Інформація о клієнтах	Обмежений	Конфіденційна інформація	Бізнес аналітики, менеджери департаменту працюючого із клієнтом, топ менеджери
Щоденні звіти	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Місячні звіти	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Бухгалтерська документація	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, бухгалтери, працівники яких стосується документація
Інформація о працівниках	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаментів, працівники відділу кадрів.
Внутрішні розпорядження	Обмежений	Конфіденційна інформація	Всі працівники підприємства, для яких призначене розпорядження
Ділова переписка із клієнтами	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом, працівники що ведуть переписку
Внутрішня ділова переписка	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, працівники що ведуть переписку

Продовження таблиці 2.4

Інформація	Режим доступу	Правовий режим	Співробітник, маючий доступ
Результаті бізнес аналізу проектів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом
Інформаційні ресурси проектів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери
Загальна інформація о підприємстві, статут підприємства	Не обмежений	Відкрита інформація	

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

Таблиця 2.5 – Аналіз інформаційних потоків типового підприємства

Інформація	Режим доступу	Правовий режим	Співробітник, маючий доступ
Внутрішня ділова переписка	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, працівники що ведуть переписку
Ділова переписка із клієнтами	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту відповідального за працівників, бізнес аналітики працюючи з даним клієнтом, працівники що ведуть переписку
Звітування місячних та денних звітів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери департаменту працюючого із клієнтом, співробітник відповідальний за звіт
Звітування аналітичних звітів	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, працівники які складають звіт

Продовження таблиці 2.5

Інформація	**Режим доступу**	**Правовий режим**	**Співробітник, маючий доступ**
Розробка та поширення інформаційних ресурсів проекту	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, працівники що розроблюють інформаційні ресурсі
Узгодження проектної документації	Обмежений	Конфіденційна інформація	Клієнти, менеджери, співпрацівники що розроблюють проектні плани та документацію
Узгодження бухгалтерської документації	Обмежений	Конфіденційна інформація	Топ менеджери, менеджери, менеджери, бухгалтери, працівники яких стосуються документація
Презентації проектів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери
Командний аналіз проектних планів	Обмежений	Конфіденційна інформація	Персонал що безпосередньо працює з проектом, топ менеджери

2.5 Аналіз загроз безпеці ІТС підприємства

2.5.1 Поняття загрози інформаційній безпеки підприємства

Криміногенний стан в країні, наявність жорсткої конкуренції та потужних фінансових потоків та технічної озброєності підприємств дає підставу до зріст ризиків інформаційної безпеки комерційних підприємств. Звідси визначення і прогнозування можливих загроз і усвідомлення їх небезпеки необхідні для обґрунтування, вибору і реалізації захисних заходів, адекватних загрозам інтересам підприємства.

Поняття загрози розуміється як потенційно можливі або реальні дії зловмисників чи конкурентів, здатні нанести матеріальної або моральної шкоди.

Загроза інформаційній безпеці ІС – сукупність умов і чинників, що створюють небезпеку несанкціонованого доступу до інформації, циркулюючої в ав-

томатизованій системі, а також можливі наслідки дій порушника на ІС підприємства, не запобігання, не виявлення і не ліквідація якого може привести до погіршення заданих якісних характеристик функціонування ІС або порушенню її працездатності, а також спотворенню і витокам інформації.

2.5.2 Джерела загроз

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІС.

Загрози та їх джерела (в т.ч. зловмисники), методи і засоби захисту і підходи до оцінки ефективності можна розрізнити відповідно до рівню ІТС є різними. Тому для ефективного функціонування ІТС та ведення інформаційної безпеки, необхідно розподілити інформацію за рівнями інформаційної інфраструктури.

Рівні інформаційної інфраструктури:

– операційних систем;

– мережевих додаткових програм і сервісів;

– систем управління базами даних;

– фізичний (лінії зв'язку, апаратні засоби та ін.);

– мережевого устаткування (мережеві апаратні засоби: маршрутизатори, комутатори, концентратори та ін.);

– бізнес-процесів організації.

Джерела загроз на фізичного, мережевого та рівня мережевих додаткових програм:

– зовнішні джерела загроз: особи, що поширюють віруси і інші шкідливі програми, хакери і інші особи, що здійснюють НСД;

– внутрішні джерела загроз: особи, що реалізовують загрози в рамках своїх повноважень і за їх межами (персонал, що має права доступу до апаратного устаткування, зокрема мережевому, адміністратори мережевих додаткових програм і тому подібне);

– комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють спільно і/або погоджено.

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

– внутрішні, такі, що реалізовують загрози в рамках своїх повноважень і за їх межами (адміністратори ОС, адміністратори СУБД, адміністратори ІБ і так далі);

– комбіновані джерела загроз: зовнішні і внутрішні, такі, що діють в змові.

Джерела загроз на рівні бізнес-процесів:

– внутрішні джерела, що реалізовують загрози в рамках своїх повноважень і за їх межами (авторизовані користувачі і оператори АБС, представники менеджменту організації і ін.);

– комбіновані джерела загроз: зовнішні (наприклад, конкуренти) і внутрішні, такі, що діють в змові.

2.5.3 Класифікація загроз інформаційним ресурсам підприємства

Першочерговою задачею для успішного ведення діяльності ІТ підприємства, як зазначалося вище, є підтримання стабільного функціонування ІТС та забезпечення безпеки циркулюючих інформаційних потоків.

На рисунку 2.2 представлені базові загрози, які мають вплив на конфіденційність, цілісність та доступність інформаційних ресурсів.

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

2.5.3.1 Загрози порушення конфіденційності

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом. Конфіденційність передбачає забезпечення захисту даних, що передаються, від пасивних атак, тобто захист потоку даних від можливості його аналітичного дослідження.

Рисунок 2.2 – Базові загрози безпеці інформаційних ресурсів

До загроз порушення конфіденційності інформації відносять розкрадання (копіювання) і витоки інформації. Основними видами атак направлених на порушення конфіденційності є пасивне підслуховування і перехоплення в каналах зв'язку, незаконне використання прав, викрадання ключової інформації.

Витоки/втрати інформації підривають авторитет компаній і завдають величезні збитки. За даними аналітиків, найближчими роками світовий корпоративний сектор нестиме втрати приблизно $1 трлн. щорічно внаслідок витоку конфіденційних даних.

2.5.3.2 Загрози порушення цілісності

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Загрози цілісності даних, програм, апаратури. Цілісність даних і програм порушується при несанкціонованому знищенні, додаванні зайвих елементів і модифікації записів про стан рахунків, зміні порядку розташування даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, при

активній ретрансляції повідомлень з їх затримкою. Несанкціонована модифікація інформації про безпеку системи може привести до несанкціонованих дій (невірній маршрутизації або втраті даних, що передаються) або спотворення сенсу повідомлень, що передаються. Цілісність апаратури порушується при її пошкодженні, викраданні або незаконній зміні алгоритмів роботи.

2.5.3.3 Загрози порушення доступності

Доступність – властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Загрози доступності даних виникають у тому випадку, коли об'єкт (користувач або процес) не дістає доступу до законно виділених йому служб або ресурсів. Ця загроза реалізується захопленням ресурсів, блокуванням ліній зв'язку несанкціонованим об'єктом в результаті передачі по ним своєї інформації або виключенням необхідної системної інформації. Ця загроза може привести до ненадійності або поганої якості обслуговування в системі і, отже, потенційно впливатиме на достовірність і своєчасність доставки платіжних документів.

Відповідно до вимог стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010, інформаційна безпека передбачає збереження конфіденційності, цілісності та доступності інформації, і може враховувати інші властивості такі, як автентичність, спостержність, неспростовність та надійність.

Автентичність – властивість, яка гарантує, що суб’єкт або ресурс ідентичні заявленим.

Спостереженість – властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Неспростовність – здатність засвідчувати дію або подію, яка мала місце так, щоб ці події або дії не могли бути пізніше спростовані. (ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції та моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT))

На рисунку 2.2 наведена модель реалізації загроз з урахуванням джерел загроз, вразливостей та методів реалізації загроз інформаційній безпеці.

Загрози інформаційним ресурсам виявляються у вигляді:

– розголошування конфіденційної інформації;

– витоків конфіденційної інформації через технічні засоби забезпечення виробничої діяльності різного характеру і виконання;

– несанкціонованого доступу до відомостей, що охороняються, з боку конкурентних організацій і злочинних формувань.

Здійснення загроз інформаційним ресурсам може бути проведене:

– шляхом неофіційного доступу і знімання конфіденційної інформації;

– шляхом підкупу осіб, що працюють в банці або структурах, безпосередньо пов'язаних з його діяльністю;

Рисунок 2.3 – Модель реалізації загроз

– шляхом перехоплення інформації, циркулюючої в засобах і системах зв'язку і обчислювальної техніки за допомогою технічних засобів розвідки і знімання інформації, несанкціонованого доступу до інформації і навмисних програмно-математичних дій на неї в процесі обробки і зберігання;

– шляхом підслуховування конфіденційних переговорів, що ведуться в службових приміщеннях, службовому і особистому автотранспорті і т.д.;

– через переговорні процеси між підприємством і іноземними або вітчизняними фірмами, використовуючи необережне поводження з інформацією;

– через окремих співробітників підприємства, прагнучих дістати більший, ніж їх зарплата, дохід або що мають іншу корисливу або особисту зацікавленість.

За ознакою джерела загрози безпеці комерційної установи вирізняються:

– загрози з боку конкурентів, тобто вітчизняних та зарубіжних підприємств, які прагнуть до посилення власних позицій на відповідному ринку шляхом використання заходів недобросовісної конкуренції, наприклад економічного шпіонажу, переманювання висококваліфікованих співробітників, дискредитації суперника в очах партнерів та держави;

– загрози з боку кримінальних структур і окремих зловмисників, що прагнуть до досягнення власних цілей, які знаходяться в протиріччі з інтересами конкретного підприємства, наприклад, захоплення контролю над ним, розкрадання власності, нанесенню іншого збитку;

– загрози з боку нелояльних співробітників підприємства, які усвідомлено наносять збиток заради досягнення власних цілей, наприклад, поліпшення матеріального становища, кар’єрного росту, помсти працедавцю за реальні або уявні образи та ін.

За видами можливих джерел загроз ІБ виділяються наступні класи загроз:

– загрози, пов'язані з навмисними або ненавмисними діями осіб, що мають доступ до ІС, включаючи користувачів ІС, що реалізовують погрози безпосередньо в ІС (внутрішній порушник);

– загрози, пов'язані з навмисними або ненавмисними діями осіб, що не мають доступу до ІС, що реалізовують погрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну (зовнішній порушник).

За видами несанкціонованих дій, здійснюваних з інформаційними ресурсами виділяються наступні класи загроз:

– загрози, що призводять до порушення конфіденційності ІР (копіюванню або несанкціонованому розповсюдженню|), при реалізації яких не здійснюється безпосередньої дії на зміст інформації;

– загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на зміст інформації, в результаті якого здійснюється зміна ІР або їх знищення;

– загрози, що призводять до несанкціонованого, зокрема випадкового, впливу на програмні або програмно-апаратні елементи ІС, в результаті якого здійснюється блокування ІР.

За оцінкою вітчизняних і зарубіжних дослідників персонал є важливим внутрішнім джерелом ризику ухвалення помилкових рішень і протиправної поведінки, у тому числі і у зв'язку з діями інших осіб і організацій з примусу співробітників до злочинної діяльності. При цьому можливі спроби впровадження в кадровий склад представників кримінальних і інших не дружніх підприємству організацій.

2.6 Моделі загроз і порушника ІБ

Моделі загроз і порушників ІБ розробляються, як правило, для підприємств в цілому, але при необхідності можлива розробка для окремих процесів при цьому ступінь деталізації параметрів моделей загроз і порушників ІБ може бути різна.

2.6.1 Модель загроз

Відповідно до вимог до забезпечення інформаційної безпеки автоматизованої системи визначені наступні моделі загроз:

– навмисні програмно-технічні впливи (дії) з метою порушення цілісності (знищення, спотворення) інформації в процесі її обробки, передачі і зберігання в ІС;

– порушення санкціонованої доступності інформації в ІС, за рахунок порушення працездатності програмного забезпечення, комунікаційного устаткування і маршрутизаторів ІС або їх перепрограмування (дефекти, збої, аварії і відмови апаратно-програмних комплексів);

– витік і спотворення конфіденційної інформації за рахунок несанкціонованого доступу до неї через технічні засоби ІС, витік конфіденційної інформації по технічних каналах;

– розголошування конфіденційної інформації і неправомірні дії з боку осіб, що мають право доступу до конфіденційної інформації і реалізовують загрози в рамках своїх повноважень і за їх межами.

Таблиця 2.6 – Загальна модель загроз безпеці інформаційних ресурсів

Джерело загрози безпеці КІ	**Рівень реалізації загрози безпеці КІ**	**Типи об'єктів середовища**	**Загроза безпеці ІзОД**
Комп'ютерні зловмисники, що здійснюють цілеспрямовану деструктивну дію	ОС	Файли даних з ІзОД	К, Ц, Д
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, ПК	К, Ц, Д
Постачальники програмно-технічних засобів, витратних матеріалів, послуг і т.п., підрядчики, що здійснюють монтаж, усконалагоджувальні роботи устаткування і його ремонт	ОС	Файли даних з ІзОД	К, Ц
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, ПК	К, Ц

Продовження таблиці 2.6

Джерело загрози безпеці КІ	**Рівень реалізації загрози безпеці КІ**	**Типи об'єктів середовища**	**Загроза безпеці ІзОД**
Співробітники, що діють в рамках наданих повноважень	Фізичний рівень	Лінії зв'язку, апаратні і технічні засоби, сервера, фізичні носії інформації, маршрутизатори, комутатори, концентратори, програмні компоненти передачі даних по комп'ютерних мережах (мережеві сервіси)	К, Ц, Д
	ОС	Файли даних з ІзОД	К, Ц, Д
	ПЗ	Бази даних з ІзОД, прикладні програми доступу і обробки ІзОД, програмні компоненти передачі даних по комп'ютерних мережах	К, Ц, Д
Співробітники, що діють поза рамками наданих повноважень	ОС	Файли даних з ІзОД	К, Ц
	ПЗ	Бази даних з ІзОД Прикладні програми доступу і обробки ІзОД	К,Ц

Основними критичними елементами засобів автоматизації ІС (в порядку спадання їх важливості) є:

– сервера баз даних і додаткових програм|;

– комунікаційне устаткування| (компоненти) системи передачі даних (маршрутизатори, концентратори, модеми);

– спеціалізовані АРМ зі встановленими СКЗІ;

Об'єктами захисту засобів автоматизації є:

– програмно-технічний комплекс АС

– в цілому як автоматизована система, що оброблює конфіденційну інформацію;

– сервера баз даних і додаткових програм;

– спеціалізованих АРМ зі встановленими СКЗІ;

– робочі станції кінцевих користувачів ІС;

– канали зв'язку, за допомогою яких здійснюється інформаційний обмін в ІС;

– приміщення, в яких розташовується серверна частина програмно-технічних комплексів і робочі станції кінцевих користувачів (залежно від оброблюваної інформації).

Система інформаційної безпеки ІС будується відповідно до певного характеру загроз і основних елементів системи, на які ці загрози розповсюджуються.

2.6.2 Модель порушника

Джерелами загроз НСД в ІС можуть бути:

– порушник;

– носій шкідливої програми;

– апаратна закладка.

Зовнішніми порушниками можуть бути:

– розвідувальні служби держав;

– кримінальні структури;

– конкуренти (конкуруючі організації);

– недобросовісні партнери;

– зовнішні суб'єкти (фізичні особи).

Зовнішній порушник має наступні можливості:

– здійснювати несанкціонований доступ до каналів зв'язку, що виходять

– за межі службових приміщень;

– здійснювати несанкціонований доступ через автоматизовані робочі місця, підключені до мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну;

– здійснювати несанкціонований доступ до інформації з використанням спеціальних програмних дій за допомогою програмних вірусів, шкідливих програм, алгоритмічних або програмних закладок;

– здійснювати несанкціонований доступ через елементи інформаційної інфраструктури ІС, які в процесі свого життєвого циклу (модернізації, супроводу, ремонту, утилізації) виявляються за межами контрольованої зони;

– здійснювати несанкціонований доступ через інформаційні системи взаємодіючих відомств, організацій і установ при їх підключенні до ІС.

Внутрішніми порушниками можуть бути:

– особи, що мають санкціонований доступ в контрольовану зону, але не мають доступу до ІР;

– зареєстрований користувач інформаційних ресурсів, що має обмежені права доступу до ІС з робочого місця;

– користувачі інформаційних ресурсів, що здійснюють віддалений доступ до ІР по ЛОМ;

– зареєстрований користувач з повноваженнями системного адміністратора ІС;

– зареєстрований користувач з повноваженнями адміністратора безпеки ІС;

– програмісти-розробники прикладного ПЗ і осіб, що забезпечують його супровід в ІС;

– розробники і особи, що забезпечують постачання, супровід в ІС.

Можливості внутрішнього порушника істотним чином залежать від тих, що діють в межах контрольованої зони режимних і організаційно-технічних заходів захисту, зокрема по допуску фізичних осіб до ІР і контролю порядку проведення робіт.

В залежності від можливостей, внутрішніх потенційних порушників можна представити у вигляді наступної ієрархії рівнів (кожний наступний рівень включає в себе функціональні можливості попереднього):

– перший рівень – визначається можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень – визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень – визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень – визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення ІС, аж до включення до складу ІС власних засобів з новими функціями обробки інформації.

За рівнем знань про ІС всіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості ІС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації ІС;

– володіють інформацією про функції та механізм дії засобів захисту.

Класифікація порушників за рівнем можливостей та рівнем знань наведена згідно НД ТЗІ 1.4-001-2000 Типового положення про службу захисту інформації.

2.7 Аналіз загроз витоків інформаційних ресурсів ІТ підприємства

В дипломній роботі створення моделі загроз реалізовуватиметься з урахуванням найбільш значної загрози витокам інформаційних ресурсів в ІТ підприємстві – навмисних або ненавмисних дій внутрішніх порушників.

В таблиці 2.7 представлена модель загроз безпеці інформаційних ресурсів, джерелом яких є навмисні та ненавмисні дії персоналу.

Таблиця 2.7 – Модель загроз безпеці інформаційним ресурсам

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Загрози несанкціонованого доступу до інформації		
Загрози знищення, розкрадання носіїв інформації шляхом фізичного доступу до елементів ІС		
Крадіжка носіїв інформації	Середня	Висока
Крадіжка ключів доступу	Висока	Висока
Крадіжки, модифікації, знищення інформації.	Висока	Висока
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	Низька	Середня
Несанкціоноване відключення засобів захисту	Висока	Висока
Загрози навмисних дій внутрішніх порушників		
Витік даних від порушення експлуатації програмного забезпечення	Висока	Висока
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	Висока	Висока
Передача конфіденційної інформації, з використанням електронної пошти	Висока	Висока
Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока
Передача нешифрованої інформації, що захищається, в зовнішню мережу	Середня	Висока
Передача зашифрованої інформації, що захищається, в зовнішню мережу	Середня	Середня
Витік інформації за рахунок запису інформації, що захищається на знімні носії (USB накопичувачі і т. д.)	Середня	Висока
Витік інформації за рахунок друку документів, які містять конфіденційну інформацію	Висока	Висока
Компрометація інформації за допомогою шахрайського копіювання даних	Висока	Висока
Компрометація інформації за допомогою нелегального оброблення даних	Висока	Висока
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	Середня	Висока
Компрометація інформації за рахунок підробки прав доступу до інформації	Середня	Середня
Доступ, модифікація, знищення інформації особами, не допущеними до її обробки	Висока	Висока
Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	Висока	Висока

Продовження таблиці 2.7

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Загрози ненавмисних дій користувачів і порушень безпеки функціонування		
Витік даних від недбалості персоналу	Висока	Висока
Витік даних від порушення експлуатації обладнання/ програмного забезпечення	Середня	Висока
Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	Середня	Висока
Втрата ключів доступу	Висока	Висока
Ненавмисна модифікація (знищення) інформації співробітниками	Висока	Висока
Ненавмисне відключення засобів захисту	Низька	Середня

Функція імовірності реалізації певної загрози, виду і величини завданих збитків визначає ризик для безпеки інформаційних ресурсів підприємства.

Процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС визначається як аналіз ризику.

2.8 Порівняння моделі загроз із використанням DLP-системи в ІТС та без

В таблиці 2.8 наведена модель загроз безпеці інформаційних ресурсів із впровадження системи захисту від витоків на основі DLP.

Таблиця 2.8 – Модель загроз безпеці інформаційних ресурсів із впровадження системи захисту від витоків на основі DLP

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Загрози несанкціонованого доступу до інформації		
Загрози знищення, розкрадання носіїв інформації шляхом фізичного доступу до елементів ІС		
Крадіжка носіїв інформації	Середня	Висока
Крадіжка паперових носіїв інформації	Висока	Висока
Крадіжка ключів доступу	Висока	Висока

Продовження таблиці 2.8

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Крадіжки, модифікації, знищення інформації.	Середня	Висока
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищенні) вузлів ПЕОМ	Середня	Середня
Несанкціоноване відключення засобів захисту	Висока	Висока
Загрози навмисних дій внутрішніх порушників		
Витік даних від порушення експлуатації програмного забезпечення	Середня	Висока
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	Висока	Висока
Передача конфіденційної інформації, з використанням електронної пошти	Низька	Висока
Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока
Передача нешифрованої інформації, що захищається, в зовнішню мережу	Низька	Висока
Передача зашифрованої інформації, що захищається, в зовнішню мережу	Низька	Середня
Витік інформації за рахунок запису інформації, що захищається, на знімні носії (USB-накопичувачі і т.д.)	Низька	Висока
Витік інформації за рахунок друку документів, які містять конфіденційну інформацію	Низька	Висока
Компрометація інформації за допомогою шахрайського копіювання даних	Низька	Висока
Компрометація інформації за допомогою нелегального оброблення даних	Середня	Висока
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	Середня	Висока
Компрометація інформації за рахунок підробки прав доступу до інформації	Середня	Середня
Доступ, модифікація, знищення інформації особами, не допущеними до її обробки	Середня	Висока
Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	Середня	Висока
Загрози ненавмисних дій користувачів і порушень безпеки функціонування		
Витік даних від недбалості персоналу	Низька	Висока
Витік даних від порушення експлуатації обладнання/ програмного забезпечення	Середня	Висока
Витік даних від неавторизованого використання обладнання/програмного забезпечення	Середня	Висока

Продовження таблиці 2.8

Перелік загроз	**Імовірність реалізації загрози**	**Небезпека загрози**
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	Низька	Висока
Втрата ключів доступу	Висока	Висока
Ненавмисна модифікація (знищення) інформації співробітниками	Середня	Висока
Ненавмисне відключення засобів захисту	Низька	Середня

Під небезпекою загрози розуміється її можливий вплив на безпеку інформаційних ресурсів підприємства, який може привести до негативних наслідків.

На рисунку 2.3 наведена порівняльна характеристика ймовірностей реалізації загроз безпеці інформаційних ресурсів від ненавмисних дій внутрішніх порушників, До та Після впровадження DLP-системи, яка відображає ефективність використання системи протидії витокам конфіденційної інформації на основі DLP.

За результатами порівняльного аналізу, спостерігається значне зниження імовірності реалізації загроз ненавмисних дій персоналу в результаті необережних дій/недбалості, а також помилок при обробці інформації.

На рисунку 2.4 наведена порівняльна характеристика ймовірностей реалізації загроз безпеці інформаційних ресурсів від навмисних дій внутрішніх порушників, До та Після впровадження DLP-системи, яка відображає ефективність використання системи протидії витокам конфіденційної інформації на основі DLP.

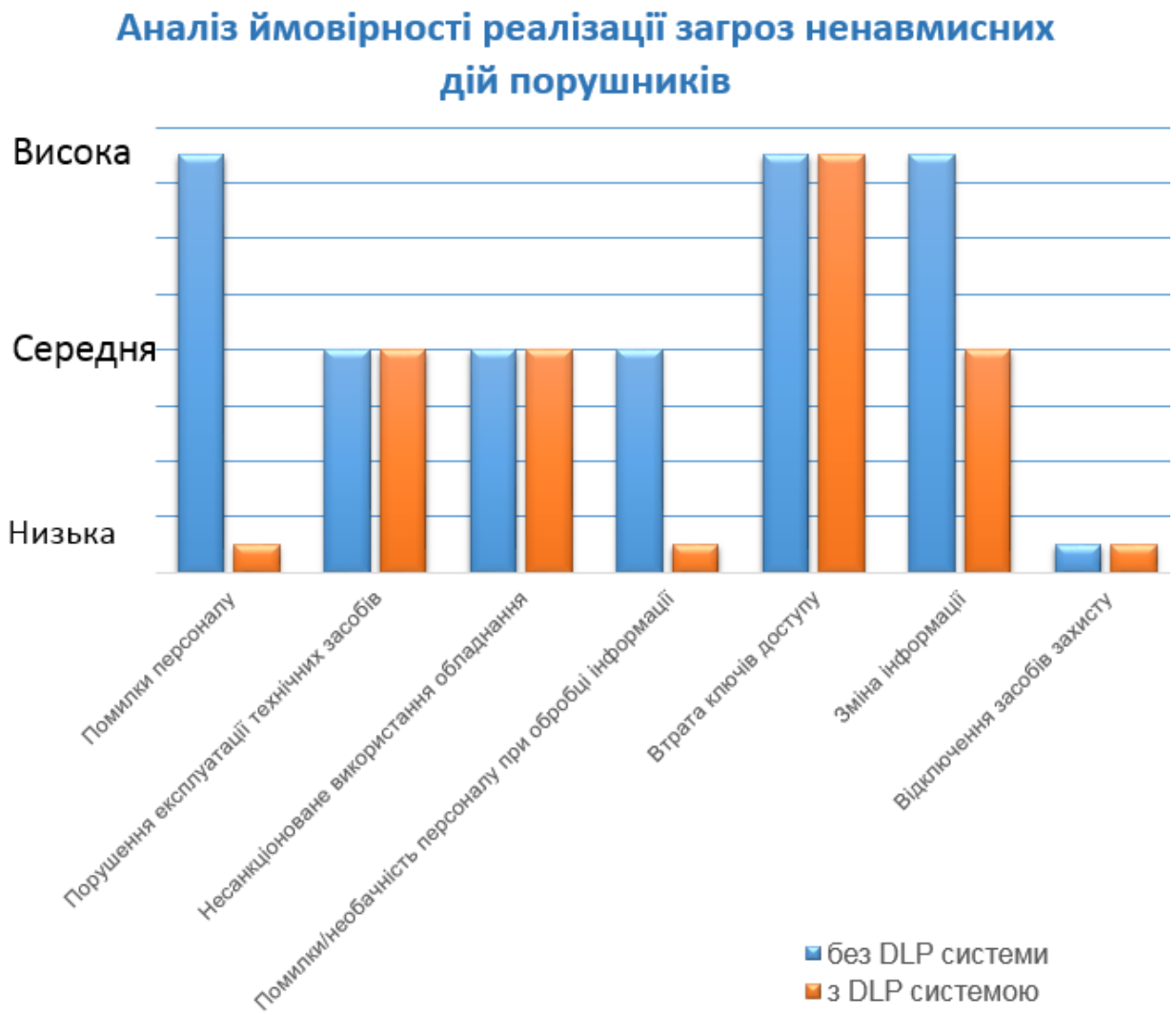


Рисунок 2.4 – Порівняльний аналіз ймовірностей реалізації загроз від ненавмисних дій внутрішніх порушників

Результати порівняльного аналізу відображають значне зниження імовірності реалізації загроз навмисних дій персоналу по напрямах:

– передача КІ з використанням електронної пошти;

– передача шифрованої інформації в зовнішню мережу;

– передача нешифрованої інформації в зовнішню мережу;

– запис КІ на з’ємні носії;

– друк документів, які містять КІ;

– шахрайське копіювання даних.

Також спостерігається зниження імовірності реалізації загроз, пов’язаних з модифікацією, знищенням, нелегальним обробленням інформації.

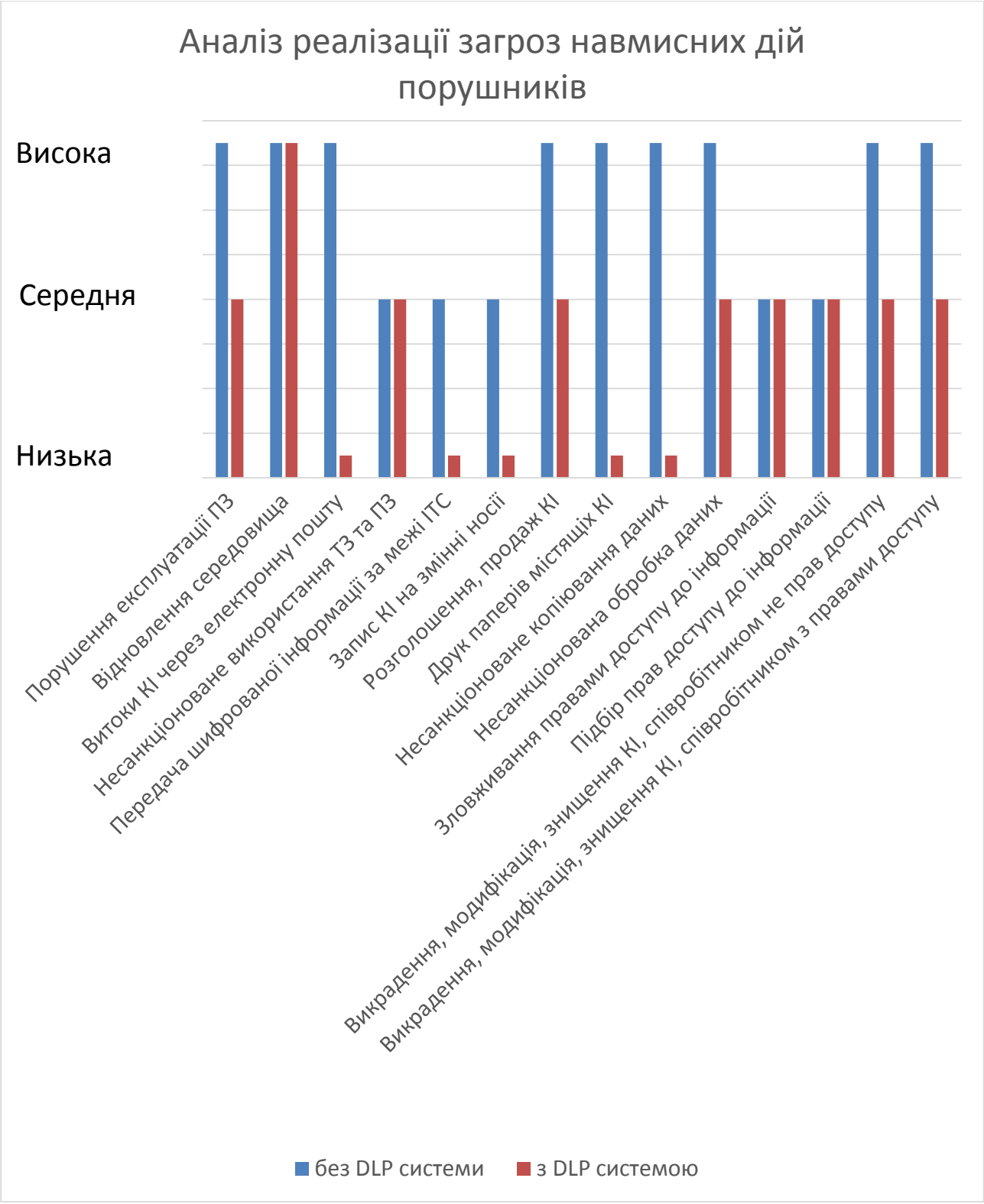


Рисунок 2.5 – Порівняльний аналіз ймовірностей реалізації загроз від навмисних дій внутрішніх порушників

2.9 Висновок

У другому розділі 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.

Розглянуті моделі забезпеченні ІБ мають позитивний вплив на стан інформаційної безпеки у межах ІТС підприємства.

Враховуючи динаміку розвитку ІТС сучасних підприємств, а також інформаційно-телекомунікаційні потреби сучасного бізнесу та великого об’єму даних, якій знаходяться в обігу, використання засобів захисту інформації є необхідною умовою існування підприємства.

Використання традиційних рішень інформаційної безпеки не забезпечує достатнього рівня захищеності від існуючих і нових виникаючих загроз інформаційній безпеці від внутрішніх порушників. Використання моделей ІБ заснованих на DLP-систем є одним з ефективних заходів по запобіганню витоку конфіденційної інформації.

DLP-система розглядається у якості складової частини КЗЗ, метою якої є мінімізація ризиків прямих і непрямих фінансових наслідків витоку конфіденційної інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Розрахунок капітальних витрат

Інвестиції в DLP = Капітальні витрати + Постійні витрати, де в капітальні витрати включаються витрати на дослідження, проектування, закупівлю ПЗ та інше обладнання, а в постійні витрати – технічна підтримка встановленого обладнання і ПЗ, продовження ліцензій, додаткові витрати на адміністрування (тестування і настройку) і експлуатацію.

Повна комплектація DLP-системи «КІБ СёрчІнформ» (включаючи 1 рік техпідтримки, впровадження та навчання фахівців) залежить від кількості хостів області контролю і для 100 ПК складає приблизно 630 тис. грн.

Вартість обладнання і системного ПЗ – 34 тис. грн. (вартість сервера для 100 агентів) і ~ 4,5 тис. грн. (вартість системного ПЗ: Windows 2008 R2, Microsoft SQL Server 2008 R2 Standard).

У підсумку отримуємо ~ 38,5 тис. грн. для 100 агентів.

При придбанні DLP-системи «КІБ СёрчІнформ» перший рік технічну підтримки входить у вартість ліцензії. Надалі щороку оплата становить 30% від вартості ліцензій. Таким чином, для 100 машин вартість техпідтримки складе ~ 189 тис. грн. в рік, починаючи з другого року експлуатації системи.

У техпідтримку буде входити:

• оновлення софту (випуск нових версій, розширення функціоналу, оптимізація роботи, виправлення багів і т.д.);

• обслуговування по інженерній частині (наприклад, якщо клієнт з якоїсь причини не може або не знає, як розбити індекси, налаштувати автоматичний запуск компонент, прописати альтернативні адреси серверів і т.д.);

• первинне навчання за частиною аналітики (створення та налаштування політик, складання звітів і т.д.) і подальша підтримка з боку відділу впровадження розробника.

Роботи по впровадженню DLP-системи зазвичай включають:

• заповнення анкети (для визначення складу обладнання, ПЗ та планування робіт);

• підготовка до тестового впровадження;

• тестове впровадження (може включати порівняльні випробування, тестування навантаження і т.п.);

• розгортання (установка) DLP-системи;

• первинне навчання;

• настройка політик безпеки;

• аналіз перехопленої інформації та формування звітів.

Вартість цих робіт, в даному випадку, включена в зазначену вище вартість ліцензії. У загальному випадку для DLP-систем вона може в середньому становити близько 10-20% від вартості продукту.

Функціонування DLP-системи має підтримуватися комплексом організаційних і юридичних заходів, документування яких здійснюється в ході розробки комплекту організаційно-розпорядчих документів. Приблизний перелік витрат наведено в табл. 3.1.

Таблиця 3.1 – Вартість розробки комплектації DLP-системи для 100 ПК

№ п/п	Найменування показника	Трудомісткість, люд./год	Вартість, тис. грн.
1	Обстеження, інвентаризація інформактивів	20	-
2	Розробка політики забезпечення конфіденційності інформації	10	-
3	Розробка політики та регламентну управління інцидентами ІБ	10	-
4	Розробка політики допустимого використання ресурсів корпоративної мережі та правил роботи користувачів	8	-

Продовження таблиці 3.1

№ п/п	Найменування показника	Трудомісткість, люд./год	Вартість, тис. грн.
5	Розробка положення о запобігання витоку інформації	8	-
6	Розробка інструкції адміністратору DLP-системи	6	-
7	Розробка інструкції експерту-аналітику по налаштування правил фільтрації контенту	6	
8	Розробка форм звітності по запобіганню витоку інформації та по інцендентам	5	
	Всього	73	65700

3.2 Поточні витрати

Тепер порахуємо вартість володіння для DLP-системи на 5-річний період для 100 ПК (див. табл. 3.2.)

Таблиця 3.2 – Вартість обслуговування DLP- системи

Стаття витрат	Сума, тис. грн.
Ліцензія на DLP-систему	630
Серверне обслуговування та системне ПО	36
Технічна підтримка DLP-системи на 4 роки	746
Розробка ОДР для DLP-системи	66
Витрати на навчання (2 спеціаліста на 7 днів)	10
Обслуговування DLP-системи (заробітна плата 1 спеціаліста на 5 років)	620
Всього	2108

Таким чином обслуговування DLP-системи «КІБ СёрчІнформ» становить 2108 тис. грн. на 100 машин на 5-річний період або 422 тис. грн на рік.

3.3 Оцінка наслідків витоків інформації

Середньостатистична вартість витоків може бути порівнянною із середньомісячним оборотом підприємства.

Вплив репутаційного збитку на прибуток підприємства показано в табл.3.3. Прямі витрати і репутаційні втрати підсумовуються. Отримуємо цифри по недоотриманого прибутку на 5-річний період.

Таблиця 3.3 – Оцінка впливу витоку на прибутковість підприємства середнього розміру

Показники в тис. грн.	**1-й рік**	**2-й**	**3-й**	**4-й**	**5-й**
Річний виторг (передбачається 8% зростання)	1,000,000	1,080,000	1,166,400	1,259,712	1,360,488
Річний чистий прибуток (передбачається маржінальність 20%)	200,000	216,000	233,280	251,942	272,097
Річна вартість ліквідації наслідків витоку	12,220	8,450	5,770	4,680	4,680
втрати бізнесу	120,000	129,600	139,968	151,165	163,258
Сумарні втрати від витоку	132,220	138,050	145,738	155,845	167,938
Результуючий річний чистий прибуток	67,780	77,950	87,542	96,096	104,159
Зменшення прибутковості із-зі витоку	66%	64%	62%	62%	62%

Оціночна вплив на рентабельність підприємства приведені в табл. 3.3 порівняння рентабельності:

• річний чистий прибуток (передбачається 20% маржі);

• річний чистий прибуток (з урахуванням втрат від витоку).

Тепер потенційний збиток від витоку можна порівняти з вартістю DLP-системи. Як вартості DLP-системи береться вартість підписки на Websense Data Protect (один з лідерів світового ринку DLP-систем) на 100 000 користувачів.

Таблиця 3.4 – Вартість DLP-системи у відсотках від можливого загального розміру збитку

Показники в тис. грн.	1-й рік	2-й	3-й	4-й	5-й
Сумарні втрати від витоку	132,220	138,050	145,738	155,845	167,938
Сумарна вартість DLP-системи	385	193	192	191	191
Вартість DLP-системи у відсотках від загального розміру збитку	0.29%	0.14%	0.13%	0.12%	0.11%

З таблиці видно, що в середньому це співвідношення становить 0,15%. Ця цифра відповідає розмірам страхової премії, в разі, якщо ми розглядаємо витрати на ІБ як страхування від відповідних ризиків.

3.4 Висновки

Таким чином, ми отримали оцінку потенційного збитку від інцидентів ІБ і оцінку вартості володіння для DLP-системи на п'ятирічний період. Для визначення величини ризику (ALE) і відповідного значення коефіцієнта повернення інвестицій (ROI) залишилося оцінити ймовірність інцидентів (загроз). Ця ймовірність, крім усього іншого, буде залежати від налаштувань політик безпеки DLP-системи, що визначають модель загроз, від яких вона забезпечує захист.

ВИСНОВКИ

У ході виконання дипломної роботи 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.

Застосування методів та моделей забезпечення ІБ заснованих на DLP-системах є економічно доцільним а економічний ефект від впровадження та використання зазначених методів та моделей є позитивним.

СПИСОК ЛІТЕРАТУРИ

1 Глобальное исследование утечек корпоративной информации и конфиденциальных даннях, 2011. Аналитический центр InfoWatch – Москва, 2013. – 30 с.

2 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.

3 Звіт по проекту «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ. Частина 2. Основні технічні рішення», – Національна Академія Наук України, Інститут Програмних Систем – Київ, 2004. – 77 с.

4 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.

5 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – НиТ, Санкт–Петербург, 2004. – 384 с.

6 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.

7 Закон України 3855–XII від 21.01.1994 «Про державну таємницю» // Голос України – 1994. – 29 с.

8 Вікіпедія (Електронний ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org. – Заголовок з екрана.

9 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

10 Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено

законодавством України (Електронний ресурс) / Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi/control/ uk/publish/article;jsessionid=140F77BFF5167554CD3353B12F059064?art_id =78319&cat_id=39181 – Заголовок з екрана.

11 Институт компьютерных технологий / Защита информации в ПЭВМ (Електронний ресурс) / Спосіб доступу: URL: http://www.ict.com.ua/ ?lng=1&sec=8&art=41 – Заголовок з екрана.

12 Система захисту інформації ЛОЗА (Електронний ресурс) / Спосіб доступу: URL: http://avtoprom.kiev.ua/product2.html – Заголовок з екрана.

13 АНКАД – Средства защиты информации, защита государственной тайны, защита персональних даннях, шифрование (Електронний ресурс) / Спосіб доступу: URL: http://www.ancud.ru/srd.html – Заголовок з екрана.

14 Products & Services – Cisco Systems (Електронний ресурс) / Спосіб доступу: URL: http://www.cisco.com/en/US/products/index.html – Заголовок з екрана.

15 Secret Net система защиты информации от несанкционированного доступа (Електронний ресурс) / Спосіб доступу: URL: http://www.securitycode.ru/ products/secret_net – Заголовок з екрана.

16 Предотвращение утечек данных (Електронний ресурс) / Спосіб доступу: URL: http://www.sovit.net/articles/technologies/data_loss_prevention/ – Заголовок з екрана.

17 Защита от утечек даннях – DLP–решения (Електронний ресурс) / Спосіб доступу: URL: http://www.protectme.ru/infosec/dlp – Заголовок з екрана.

18 Статья DLP – DataLoss / LeakPrevention – Технологии предотвращения утечек конфиденциальной информации– TADVISER (Електронний ресурс) / Спосіб доступу: URL: http://www.tadviser.ru/index.php/Статья:DLP – Заголовок з екрана.

19 Ефременко Наталья. Онтологии в DLP – системах третьего поколения. – Information Security, №4. – 2009.

20 Векторная модель текста (Електронний ресурс) / Спосіб доступу: URL: http://www.neural.ru›dictionary/Векторная модель текста – Заголовок з екрана.

21 Никоненко А.А. Обзор баз знаний онтологического типа (Електронний ресурс) / Спосіб доступу: URL: http://lingvoworks.org.ua/index.php?option=com_content&view=article&id=57:2009–12–09–11–34–5&catid=2:misc&Itemid=3 – Заголовок з екрана.

22 В.Б. Задоров. До переосмислення деяких загальносистемних понять з метою інтеграції онтологій та комп'ютерних інформаційних систем, – Стаття, Київський національний університет будівництва і архітектури, – 2010 р.

23 Технологии применения онтологий | Онтологический инжиниринг и управление знаниями | Теория (Електронний ресурс) / Спосіб доступу: URL: http://bigc.ru/theory/km/onto_technologies.php – Заголовок з екрана.

24 Болотова В.А. Григорьев А.В. Инструментальные средства создания баз знаний на основе системы онтологій (Електронний ресурс) / Спосіб доступу: URL: http://www.masters.donntu.edu.ua/2010/fknt/bolotova/library/tez1.htm – Заголовок з екрана.

25 Рейтинг зарплат 2011 року (Електронний ресурс) / Спосіб доступу: URL: http://rada.kosiv.info/kosivs/tidings/8742–reiting–zarplat–2011–roku.html – Заголовок з екрана.

26 Microsoft Україна: програми, технології, онлайн, комп'ютери, ігри (Електронний ресурс) / Спосіб доступу: URL: http://www.microsoft.com/uk–ua/default.aspx – Заголовок з екрана.

27 Информационная безопасность: экономические аспекты (Електронний ресурс) / Спосіб доступу: URL: http://citforum.univ.kiev.ua/security/articles/sec/ – Заголовок з екрана.

ДОДАТОК А. Перелік матеріалів дипломної роботи

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Список використаної літератури.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

Презентація.pptx

ДОДАТОК Б. Відгуки керівників розділів

Б.1 Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК В. ВІДГУК

на дипломну роботу магістра на тему:

Методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології

студента групи 125м-16-1

Судариков Сергій Анатолійович

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на _ _ сторінках та містить _ _ рисунків і _ _ таблиць та _ джерел.

Метою дипломної роботи оцінка ефективності методів та моделей забезпечення інформаційною безпекою в інформаційно-телекомунікаційних системах на основі DLP технології.

У ході виконання роботи були вирішені наступні завдання: проаналізовано існуючі на ринку DLP-систем, проведено аналіз ефективності методів та моделей управління інформаційною безпекою в ІТС з використанням зазначених систем.

В економічному розділі виконаний розрахунок капітальних витрат на впровадження DLP-системи на підприємстві, розраховано експлуатаційні витрати, визначено економічну ефективність від використання системи.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор Судариков Сергій Анатолійович заслуговує на оцінку «_____» та присвоєння кваліфікації «професіонал з організації інформаційної безпеки».

Керівник дипломної роботи,
к.ф.-м.н., доц. О.Ю. Гусєв

Керівник спец. част.,
ст. викл. В.О. Святошенко

Р Е Ц Е Н З І Я

на дипломну роботу магістра на тему:

Методи та моделі забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології

студента групи 125м-16-1

Судариков Сергій Анатолійович

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на ___ сторінках, та містить ___ рисунків, __ таблиць і __ джерел.

Актуальність теми:

Використання традиційних рішень інформаційної безпеки не забезпечує достатнього рівня захищеності від існуючих і нових виникаючих загроз інформаційній безпеці від внутрішніх порушників. Використання моделей забезпечення ІБ заснованих на DLP-систем є одним з ефективних заходів по запобіганню витоку конфіденційної інформації.

DLP-система розглядається у якості складової частини КЗЗ, метою якої є мінімізація ризиків прямих і непрямих фінансових наслідків витоку конфіденційної інформації.

У роботі наведені:

- аналіз статистики витоку інформації на підприємствах;
- аналіз існуючи DLP-системи;
- аналіз методи та моделі забезпечення ІБ у ІТС;
- оцінка ефективності методів та моделей забезпечення ІБ у ІТС на основі DLP технології.

Наукова новизна полягає у застосуванні сучасних методів та моделей забезпечення інформаційної безпеки інформаційно-телекомунікаційних систем на основі DLP технології з метою підвищення рівня захищеності підприємства.

В цілому дипломна робота задовольняє усім вимогам, а її автор Судариков Сергій Анатолійович заслуговує на оцінку «_____».

Рецензент