МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021 р.

На правах рукопису
УДК 004.056:57(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система захисту інформаційних ресурсів від шкідливого програмного забезпечення

Виконавець: В.В. Литвин
Керівник: к.т.н., доцент С.В. Єгоров
Нормоконтролер: к.т.н., доцент С.В. Єгоров

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«___» _____ 2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Литвина Владислава Володимировича

1. Тема: *Система захисту інформаційних ресурсів від шкідливого програмного забезпечення*

затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.

3. Вихідні дані: проаналізувати існуючі інформаційні ресурси та системи захисту та класифікувати їх; на основі проведеного аналізу визначити підходи, методи та засоби захисту інформаційних ресурсів; розробити систему захисту інформаційних ресурсів та дослідити її.

4. Зміст пояснювальної записки: аналіз та класифікація сучасних систем інформаційних ресурсів; аналіз підходів, методів та засобів захисту інформаційних ресурсів; аналіз шкідливого програмного забезпечення та ризиків для систем захисту інформаційних ресурсів; розробка та дослідження системи захисту інформаційних ресурсів.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	14.04.2021	*Виконано*
2.	Аналіз літературних джерел	15.04.2021	*Виконано*
3.	Обґрунтування рішення	16.04.2021-18.04.2021	*Виконано*
4.	Збір інформації	19.04.2021-26.04.2021	*Виконано*
5.	Аналіз шкідливого програмного забезпечення для систем захисту інформаційних ресурсів	27.04.2021-05.05.2021	*Виконано*
6.	Дослідження підходів, методів, засобів захисту інформаційних ресурсів	06.05.2021-13.05.2021	*Виконано*
7.	Розробка системи захисту інформаційних ресурсів	14.05.2021-21.05.2021	*Виконано*
8.	Дослідження системи	22.05.2021	*Виконано*
9.	Перевірка на антиплагіат	04.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	07.06.2021	*Виконано*
11.	Оформлення презентації	08.06.2021	*Виконано*
12.	Отримання рецензій	09.06.2021	*Виконано*

Здобувач вищої освіти В. Литвин

(підпис, дата)

Керівник дипломної роботи С. Єгоров

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 73 сторінки, має 34 рисунка, та має 7 таблиць. Список використаних джерел містить 32 найменування і займає 4 сторінки.

Метою дипломної роботи є підвищення рівня захищеності інформаційних ресурсів і інформації в цьому ресурсі від шкідливого програмного забезпечення.

В дипломній роботі розглянуті питання ризиків для систем захисту інформаційних ресурсів. Проаналізовані та запропоновані методи та основні напрями захисту інформаційних ресурсів.

Набула подальшого розвитку система захисту інформаційних ресурсів, що призвело до поліпшення захисту критично важливої інформації, завдяки тому, що було удосконалено методи та засоби захисту інформаційних ресурсів.

Запропонована система може використовуватися у реальних практичних СЗІ. Крім того, сформульовані практичні рекомендації будуть корисними експертам з інформаційної безпеки при прийнятті рішень щодо доцільності застосування різного роду підходів до захисту.

Ключові слова: інформаційний ресурс, система захисту інформаційних ресурсів, ризики інформаційним ресурсам, інформація, шкідливе програмне забезпечення.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІР	- інформаційний ресурс
ПЗ	- програмне забезпечення
СЗІ	- системи захисту інформації
ІТ	- інформаційні технології
КС	- комп’ютерна система
ЗІ	- захист інформації
ПК	- персональний комп’ютер
ЕОМ	- електронна обчислювальна машина
ІС	- інформаційна система
НТІР	- науково-технічні інформаційні ресурси
ЗМІ	- засоби масової інформації
БД	- база даних
ЗКЗІ	- засоби криптографічного захисту інформації
ОС	- операційна система
СІА	- система ідентифікації та авторизації
RSA	- Rivest-Shamir-Adleman- стандарт шифрування даних

ВСТУП

Актуальність. Комп'ютерні та інформаційні технології сьогодні охопили всі галузі життєдіяльності людини. Для будь-якої сучасної компанії інформація стає одним з головних ресурсів, збереження і правильне розпорядження яким має ключове значення для розвитку бізнесу і зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки допомагає захистити інформацію та інформаційну інфраструктуру підприємства від негативних впливів. Такі дії можуть носити випадковий або навмисний, внутрішній або зовнішній характер. Результатом такого втручання може стати втрата важливої інформації, її несанкціонованих змін або використання третіми особами. Тому інформаційна безпека - це важливий аспект захисту бізнесу і забезпечення його безперервності.

У діяльності будь-якої фірми є інформаційний ресурс це документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних і ІС), тобто документовані знання. Інформаційні ресурси в сучасному суспільстві відіграють не меншу, а нерідко і велику роль, ніж ресурси матеріальні. Знання кому, коли і де продати товар може цінуватися на менше, ніж товар, і в цьому плані динаміка розвитку суспільства свідчить про те, що на "терезах" матеріальних та інформаційних ресурсів останні починають переважати.

Виходячи з даних міркувань необхідне створення нових підходів до захисту інформації в інформаційних ресурсах. Це має бути новий підхід в технологіях реалізації захисту інформаційних ресурсів, а саме створення системи, за допомогою якого буде реалізовано всі необхідні механізми захисту, тобто буде створена універсальна система для захисту інформаційних ресурсів.

Метою дипломної роботи є реалізація нової системи для захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Для досягнення поставленої мети слід вирішити наступні завдання:

- проаналізувати інформаційні ресурси і класифікувати їх, дослідити існуючі підходи, засоби та методи захисту інформаційних ресурсів;
- створити систему захисту інформаційних ресурсів за допомогою фізичних, апаратних та програмних засобів забезпечення безпеки інформаційних ресурсів;
- дослідити створену систему захисту інформаційного ресурсу.

Об'єкт дослідження: процес захисту інформаційних ресурсів від шкідливого програмного забезпечення.

Предмет дослідження: апаратні та програмні системи захисту інформації.

Методи дослідження: аналіз існуючих систем захисту інформаційного ресурсу

Галузь застосування. Дана система захисту ІР може використовуватися у галузі ЗІ, зокрема системах ЗІ для підвищення ефективності захисту від шкідливого ПЗ.

Практична цінність. Набула подальшого розвитку система захисту інформаційного ресурсу, що призвело до поліпшення захисту критично важливої інформації, завдяки тому, що було удосконалено методи захисту Web-ресурсу від шкідливого програмного забезпечення, засоби автентифікації і авторизації користувачів методом двофакторної авторизації, засоби антивірусного забезпечення, а також комплекси криптографічного і міжмережевого екранування.

РОЗДІЛ 1. СУЧАСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Основні поняття інформаційного ресурсу

В ІР концентрується первинна інформація, яка відображає пізнання людства про свою емпіричну діяльність і знання про навколишнє середовище (обсяг таких знань безперервно зростає в результаті сучасних і цілеспрямованих наукових досліджень, які ведуть до відкриттів і науково-технічним досягненням, більш поглибленого і вільного освіти народу, розвитку і використання сучасних засобів обчислювальної техніки, комунікацій, зв'язку та інших факторів), а також вся вторинна інформація, яка утворюється в результаті обробки та переробки всієї отриманої інформації (яка була зафіксована на всіляких носіях протягом всього шляху історичного розвитку людства і продовжує накопичуватися і фіксуватися і в даний час) [2].

Також зазначається, що інформація, яка обробляється та зберігається, створює нову інформацію, знання, які також створить щось нове в майбутньому. Тобто можна сказати, що інформація така ж характерна, як відтворення знань та їх узагальнення, і це призведе до постійного збільшення ІР у майбутньому.

У період постіндустріального розвитку громади переваги та ефективність інтелектуальної власності посідають важливе місце завдяки своїй ефективності з точки зору важливості та розробляються як пріоритетні стратегічні ресурси, які можна порівняти з матеріальними та матеріальними енергетичними ресурсами.

Відповідно до закону "Про Національну програму інформатизації" визначення ІР звучить так:

Інформаційний ресурс - сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо)[5].

Хоча таке трактування є статичним у існуванні чи зберіганні знань і не поширюється на надзвичайно важливу інформацію, що зберігається деякими особами, які займаються певними галузями науки і техніки, медицини та біології,

літератури та мистецтв (викладачі, лікарі, вчені, інженери), раціональне визначення ІР з метою його більш широкого подання з урахуванням динамічних характеристик, що виявляються на фазах передачі та сприйняття інформації. Тоді цю концепцію можна передати наступним чином:

Інформаційний ресурс - це індивідуальні і колективні експертні знання, окремі документи, окремі масиви документів, а також документи і їх масиви, складові бази і банки даних, бази знань, бібліотеки, архіви, фонди, інформаційні системи та інші системи в певній предметній тематичної області, які задовольняють функціональним потребам і запитам споживачів інформації [1].

З огляду на вдосконалення нинішніх інформаційних технологій, перш за все поширення по всьому світу глобальної мережі Інтернет, державні кордони для інформації втрачають своє значення, і вона стає загальнодоступною для всього людства. Внаслідок цього, вся сукупність ІР, які були накопичені людьми, організаціями, регіонами, державами і використовуються на міждержавному рівні, отримала назву світових інформаційних ресурсів [4].

Історія становлення та розвитку ІР свідчить про динамічний розвиток людини як розумної істоти, яка може не лише ефективно використовувати свої інтелектуальні та духовні здібності для спілкування один з одним та активної взаємодії з природою, а й розробляти шляхи та засоби запису, зберігання, обробки та передачі інформації. У такий спосіб розвивати та вдосконалювати інформаційні технології та організовувати інформаційне середовище для їх існування.

В історії і розвитку ІР умовно виділяють наступні фази [1].

Перший етап пов’язаний із появою мови та розвитком обміну інформацією між людьми на вербальному та невербальному рівні, завдяки якому вони оцінювали різноманітний досвід людей і передавали інформацію з покоління в покоління. Вербальна, тобто словесна інформація була поштовхом для розвитку мови та пропонувала можливість створення механізмів інформаційних технологій.

Другий етап розвитку ІР відноситься до ери письменства (приблизно в

кінці IV - на початку III тисячоліття до н. е. в Єгипті та Месопотамії), коли спілкування між людьми та обмін знаннями перейшли на вищий рівень - рівень документального спілкування. Це породило технологію зберігання окремих копій інформації на примітивних носіях (папірус, глина), які можна було переміщати в просторі та часі. Існують способи доступу (хоч і невеликого, але обмеженого) до інформації поточного та історичного характеру. Саме тоді були створені перші сховища документів, що містять інформацію, що відображала стан і поведінку людей та суспільне життя.

Третій етап відзначається появою друкування (середина XI століття в Китаї, середина XV століття в Європі). Цей винахід дозволив відтворити документи у вигляді книг чи газет, поширювати їх в суспільстві, а також сформувати бібліотеки, архіви та сховища, тобто зібрати в одному місці джерела знань, що лягли в основу системи загальної та галузевої професійної освіти та поширення знань у всьому світі. Таким чином, ІР наближалася до рівня потреб людини в інформації, який, у свою чергу, зростав пропорційно.

Четвертий етап розвитку ІР відноситься до часу відкриття та застосування в технології електричних сигналів та електромагнітних хвиль (середина XIX століття). Поява телеграфів, телефонів, радіо і телебачення дозволила забезпечити швидкий обмін інформацією в будь-якому обсязі по всьому світу. На даний момент зростання обсягу генерованих ІР стало надзвичайно інтенсивним.

Це пов’язано зі швидким зростанням кількості документів, доповідей, дисертацій та звітів, що представляють результати постійно зростаючих дослідницьких і дослідно-конструкторських робіт, кількості журналів у різних сферах людської діяльності та появи різних даних (метеорологічних, геофізичних, медичних, економічних).

Така ситуація викликала новий виток бурхливого розвитку науки і техніки на базі інформаційних технологій, що пов'язано з винаходом транзистора (1947р.), мікропроцесора (1971р.) а в результаті з появою персональних комп'ютерів і комп'ютерних мереж передачі даних. Настала п'ята фаза розвитку

ІР – епоханових інформаційних технологій, що відрізняються наступними характерними рисами революційного переходу до сучасного інформаційного світу [2]:

а) заміна механічних та електричних засобів обробки інформації електронними;

б) мініатюризація всіх вузлів, пристроїв, приладів і машин, яка призвела до різкого скорочення їх енергоспоживання;

в) створення енергонезалежних елементів обчислювальних пристроїв;

г) розробка програмно-керованих пристроїв і процесорів.

Розвиток сучасних засобів зв'язку і обчислювальної техніки, створення комп'ютерних мереж в тому числі Інтернету, призвело до того, що сфера науки і освіти розширилась, також розширились і сфери впливу електронних засобів масової інформації, і, отже, до нового вибухового процесу різкого збільшення обсягу знову генеруються ІР. Так, в кінці XX - початку XXI ст. це збільшення, порівняно з попереднім періодом прийняло стрибкоподібний характер і отримало назву "інформаційного вибуху", або "інформаційної революції" [1].

Сьогодні темпи зростання інформаційних ресурсів вперше в історії людства заблокували темпи зростання потреб людини в інформації, які наближаються до своєї межі. Крім того, обсяг інформаційних ресурсів у світі продовжує зростати так само стрімко, а інформаційні потреби припинились через обмежену здатність самої людини засвоювати ці ресурси. Таким чином, епоха інформаційного насичення, або епоха інформаційної кризи, розширення якої можлива лише за допомогою науково-технічного прогресу в галузі інформаційних технологій.

В останні роки широке використання мікропроцесорів та персональних комп’ютерів, мереж передачі даних, супутникових та ефірних каналів зв'язку об’єднало світ в єдину гігантську систему, яка практично не має кордонів і забезпечує зберігання величезного різноманіття інформаційних ресурсів, поповнення та широкі можливості для їх розвитку. Розробляються нові методи, що оптимізують процеси обробки інформації (наприклад, розпаралелювання процесів), її зберігання (наприклад, стиснення) та розподілу.

Відбувається перехід до «безпаперової технології» і «безпаперового суспільству», в якому ІР представляються в основному в цифровому або електронному вигляді, а інформаційний обмін між людьми здійснюється за допомогою електронних засобів (Інтернету, електронної пошти, відеотелефона, відеоконференцій, факсимільного зв'язку). зберігання та обробка будь-якої інформації при цьому виробляється в цифровому вигляді на персональних комп'ютерах (об'єднаних розвиненою телекомунікаційною мережею), що за своєю суттю є переходом до нової - шостої фази розвитку і споживання ІР [1].

Таким чином, кінець XX ст. і початок XXI ст. знаменні розробкою нових засобів комп'ютерної обробки інформації та засобів зв'язку, що призвело до революційного етапу інформатизації суспільства.

Сучасні інформаційні технології для формування та експлуатації інтелектуальної власності призвели до створення інформаційної галузі, яка випереджає промисловість та сільське господарство за розмірами та економічними показниками.

У цей момент відбулася інформаційна індустріалізація, яка передувала зайнятості робітників, попиту, пропозиції та обміну інформаційними продуктами промислової індустріалізації. Рушійною силою суспільства є виробництво переважно інформаційних продуктів, які дають змогу виробляти матеріальні вироби в більших масштабах з точки зору інформації, маючи більше знань у галузі інноваційних рішень, у галузі виробництва, технологій економіки, а також у ринкових відносинах. Таке суспільство, в якому більшість працівників бере участь у виробництві, зберіганні, обробці та продажу інформації, називається інформаційним суспільством.

Як результат, розвиток глобальних ІР та еволюція інформаційних технологій на даний момент дозволили:

а) сформувати нові ІР на основі більш ефективних методів та засобів автоматизації та інформатизації;

б) перетворити діяльність з надання інформаційних послуг на глобальну людську діяльність;

в) сформувати світовий та внутрішній ринок інформаційних послуг;

г) створювати бази даних про ресурси регіонів і держав;

д) ефективніше використовувати існуючі ІР для підвищення обґрунтованості та ефективності управлінських рішень у технічних та організаційних та економічних системах (наприклад, фірми, банки, біржі, промисловість, торгівля), а також у соціальній та інших сферах.

Є можливість використовувати різні функції для класифікації ІР та розподілу їх на певні типи або категорії. Найзагальнішою ознакою, яка не потребує аналізу семантичних, синтаксичних чи прагматичних компонентів в ІР, є особливість форми подання або фіксації інформації.

До первинної належить, тобто такої, що відображає особливості його джерела, території чи сфери створення та його походження, включаючи інформацію, яка формується самостійно в природних умовах (наприклад, кількість кілець при спилянні дерева на його вік). Інформаційні ресурси можна класифікувати як природні, продуктивні та соціально-економічні. Одним із прикладів є інформація про приріст населення.

Інший клас інформаційних ресурсів складається з інформації, даних, штучно отриманих у процесі дослідження, та будь-яких творчих робіт. Ця інформація базується на обробці вже наявної інформації за допомогою спеціальних параметрів і моделей (математична обробка, логічна, семантична). До цього ж класу належать предмети, створені як авторські твори в галузі літератури та мистецтва. Важливою частиною цих ресурсів є інформація, отримана в результаті інтелектуальної діяльності людини. Існує вторинна інформація, яка виникає в результаті обробки існуючої інформації, і нова інформація, яка фіксує те, що людство ще не знало. Сюди входять відкриття, прогнози в галузі різних соціальних і природних процесів.

Відповідно до цієї ознаки класифікація ІР представлена на рисунку 1.1

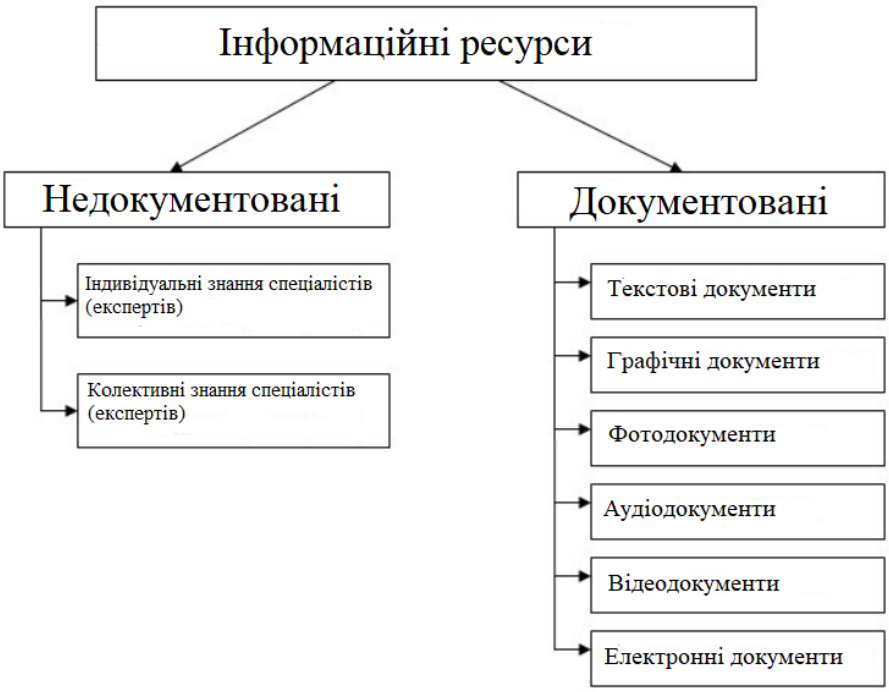

Рис. 1.1. Класифікація інформаційних ресурсів

Виходячи з наведеної класифікації, усі ІР слід розділити на два класи: недокументовані, що включає індивідуальні та колективні знання фахівців, та документовані.

Документовані ІР поділяються на текстові (письмові), графічні (малюнки, схеми, графіки, карти, діаграми, малюнки), фото-, аудіо- (записи, аудіокасети), відео- (фільми, слайди, слайди) та електронні документи.

Відповідно до права власності, інформаційні ресурси можна розділити на такі групи:

Державні (національні) інформаційні ресурси - інформаційні ресурси, що надходять і сплачуються з державного бюджету. Національні інформаційні ресурси, включаючи реєстри, кадастри, реєстри, класифікатори, створюються для швидкого доступу до повної, відповідної, достовірної та послідовної інформації про основні об'єкти, форми, методи та результати державного управління та спільного використання ними на міжвідомчому рівні органи державної влади. влади. Створення національних інформаційних ресурсів дозволяє усунути дублювання, впорядкувати та врегулювати процедури збору, зберігання та оновлення відповідної інформації, а також контролювати доступ

до них та їх використання. Ще одним видом є інформаційні ресурси підприємства.

Інформаційні ресурси підприємств - ІР, створені або накопичені на підприємствах та в організаціях. Прикладами інформаційних ресурсів підприємства є: інформаційне забезпечення господарської діяльності, планування та оперативне управління діяльністю підприємства, бізнес-плани, зовнішньоекономічна діяльність. Така інформація безпосередньо використовується підприємцями при виборі постачальників, партнерів та розміщенні замовлень; вийти на ринок з новим продуктом; знайти покупців; у злиттях та поглинаннях; для маркетингових досліджень.

Ресурси персональної інформації - ІР, створені та керовані однією або групою осіб та містять дані, пов’язані з особистою діяльністю.

На основі запису інформації задокументовані ІР також можна розділити на два класи: записані та збережені на різних типах носіїв (різні матеріали: папір, полотно, глина, парафін, плівка, плівка, магнітна плівка) та перетворені та записані в електронному вигляді. комп'ютер, дискета, компакт-диск).

Залежно від носіїв масової інформації, інформаційні ресурси поділяються на три основні класи:

-персонал зі знаннями та кваліфікацією;

-документи всіх типів та їх збори на будь-якому типі носіїв;

-колекції неживих та живих предметів (промислові зразки, рецепти та технології, типові зразки). Області застосування інформаційних ресурсів наведені в таблиці 1.1:

Таблиця 1.1

Соціально-економічні	Відомості, дані, знання, згенеровані в процесі суспільно-історичної практики людей які використовуються в економічній діяльності.

Продовження таблиці 1.1

Науково-технічні	Джерелами науково-технічних інформаційних ресурсів (НТІР) є: звіти научних робіт, дисертації, патенти, нормативно-технічна документація, інформація про експертизу продукції, огляди, покажчики літератури, реферативні журнали, неопубліковані переклади . Документальні реферативно-бібліографічні БД, створювані в результаті обробки.
Культурні	Картини, скульптури, пам'ятники, будівлі
Правові	Державна влада, інформаційно-правові бази даних, правові ЗМІ в мережі Інтернет, тематичні сайти по праву, віртуальні клуби і правові форуми, правозахисні організації та юридичні фірми, судові та правоохоронні органи
Розважальні	Соціальні мережі, месенджери, комп’ютерні ігри
Освітні	Інформаційні освітні ресурси включають широкий спектр різних об'єктів, моделей і технологій. Вони включають різні інформаційні об'єкти і комплекси: мережеві навчальні ресурси, інформаційні моделі, інтелектуальні ресурси, стандарти в галузі навчання освітні

За категорією доступу інформаційні ресурси можна поділити на такі, які наведені в таблиці 1.2.

Таблиця 1.2

відкритими	загальнодоступними
закритими	з обмеженим доступом, тобто мають конфіденційний характер або можуть бути державною таємницею

Інформація в залежності від порядку її надання або поширення поділяється на:

1)Інформацію яку можна поширювати.

Це інформація, яка не потребує жодної згоди і може вільно поширюватись через мережу Інтернет або в будь-якому іншому вигляді, в якому забажає власник цієї інформації.

2)Інформація, яка надається за згодою.

Це інформація, для поширення якої, необхідно отримати дозвіл від її власника, або від довіреної персони, яка безпосередньо знає власника

3)Інформація яка відповідно до нормативно-правовими актами підлягає наданню або поширенню.

До цієї інформації належать закони та акти, які поширюються відповідно до нормативно-правових актів.

4)Інформація поширення якої забороняється законом.

Ця інформація має назву конфіденційна інформація або державна таємниця

За характером змісту інформаційні ресурси класифікуються на:

-тематичні;

-наукові;

-новини;

-довідкові дані;

-вторинну інформацію;

-рекламу.

За ознакою тематичної приналежності інформаційні ресурси можуть бути поділені на такі підобласті, наприклад:

-наукові ресурси це можуть бути наукові статті, роботи, дослідницькі роботи;
-статистичні ресурси це ресурси про статистичні дані, тобто кількість населення для прикладу, статистика використання певних речей;
-екологічні ресурси до них відносяться об’єкти природи, навколишнє середовище;
-навчальні ресурси до них відносяться книги, презентації, тобто ресурси які використовуються у навчанні та для навчання;
-фінансово-економічні ресурси до них відносяться банківські справи, ресурси що містять економічні дані;
-нормативно-правові ресурси до них відносяться закони, положення, акти;

Також ще однією ознакою за якою можна розділити інформаційні ресурси є ознака комерціалізації, тобто отримання вигоди з інформаційного ресурсу. За цією ознакою можна виділити такі ресурси наведені в (табл. 1.3):

Таблиця 1.3

некомерційні ресурс	Бібліотеки, музеї, передачі по телебаченню
комерційні ресурси	Інформація, або ресурс, який може продаватися і має власну ціну, або платний доступ до нього.

Аналізуючи ці дані можна виділити чотири основні варіанта комерціалізації інформаційного ресурсу:
1)доступ до ресурсу надається безкоштовно, а використання його також безкоштовне;
2)доступ до ресурсу безкоштовний, використання його платне;
3)доступ до ресурсу платний, використання його безкоштовне;
4)доступ до ресурсу платний, використання його платне.

Отже, використовувати тільки один показник класифікації ІР недоцільно, так як один і той же ресурс може містити інформацію по ряду різноманітних тем. В такому випадку ІР включають до відповідних тематик або видів, і, таким чином, він може зустрічатися багаторазово.

1.2 Аналіз сучасних загроз для інформаційних ресурсів

Загрози інформаційних ресурсів це реальні або потенційно можливі дії або умови, які можуть спричинити оволодіння, розкрадання, копіювання, блокування, викривлення або зміна (модифікацію) та знищення інформації, що міститься в інформаційних ресурсах.[8]

Зазвичай існують внутрішні та зовнішні джерела загроз. Внутрішні загрози включають як навмисні дії, так і ненавмисні помилки персоналу. Зовнішні загрози дуже різноманітні. У ринковій економіці, коли існує реальна конкуренція між підприємствами, вони зацікавлені в діяльності конкуруючих організацій (фірм). Метою цього інтересу є отримання інформації, що стосується комерційної таємниці, планування, фінансового стану, клієнтів, цін. За допомогою такої інформації та її використання конкурентами (та її існуючими партнерами) є можливість отримати значну шкоду власному підприємству.

Основні загрози інформаційним ресурсам підприємства проявляються у вигляді: розголошення конфіденційної інформації; витік конфіденційної інформації через різні канали, незахищені об'єкти інформатизації:

а)основні та допоміжні технічні засоби та системи забезпечення виробничо-трудової діяльності, приміщення для конфіденційних переговорів;

б)несанкціонований доступ до захищеної інформації.

Витік конфіденційної інформації являє собою неправомірний, недозволений вихід такої інформації за межі зони, що захищається її функціонування або встановленого кола осіб, які мають право працювати з нею, якщо в результаті цього відбулося отримання інформації (ознайомлення з нею) осіб, які не мають до неї санкціонованого доступу. Прояв загроз інформаційних ресурсів підприємства може привести не тільки до витоку, але і втрати конфіденційної інформації.[9]

Уразливість інформації - це нездатність інформації самостійно протистояти дестабілізуючим впливам, тобто таким діям, які порушують її встановлений

статус. Порушення статусу будь-якої інформації полягає в порушенні її фізичної схоронності (в повному або частковому об'ємі), логічної структури та змісту, доступності для правомочних користувачів. Порушення статусу конфіденційної інформації є також порушенням її конфіденційності (закритості) для сторонніх осіб».[10]

До можливих форм прояву уразливості конфіденційної інформації підприємства, що виникають в результаті дестабілізуючого впливу на неї, належать:

1) розкрадання носія інформації або відображеної в ньому інформації;

2)втрата носія інформації;

3)несанкціоноване знищення інформації або її носія;

4)спотворення інформації (несанкціонованих змін, несанкціонована модифікація, підробка, фальсифікація);

5)блокування інформації;

6)розголошення інформації (поширення, розкриття);

7)спостереження за джерелами інформації;

8)підслуховування інформації;

9)перехоплення інформації.

1.3 Аналіз сучасного шкідливого програмного забезпечення для інформаційних ресурсів.

Шкідливе програмне забезпечення - це програмне забезпечення, призначене для заподіяння шкоди або експлуатації програмованого пристрою, послуги чи мережі. Зазвичай кіберзлочинці використовують їх для отримання даних, які вони можуть використовувати для отримання фінансової вигоди від жертв. Ці дані можуть бути інформацією від фінансових даних до медичних записів, електронних листів та паролів - будь-яка інформація може бути скомпрометована.

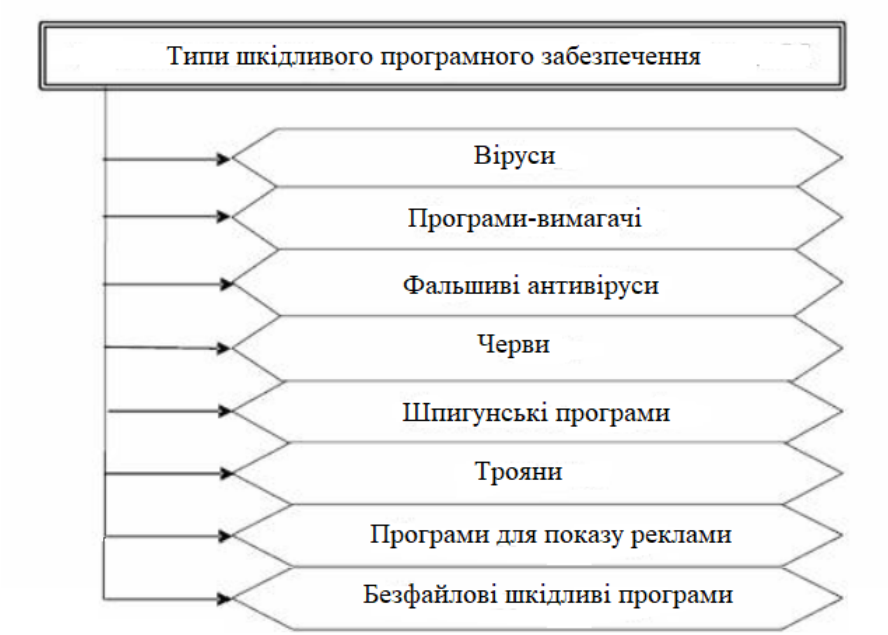

Рис. 1.2. Типи шкідливого програмного забезпечення

Віруси, які потрапляють на комп'ютер як вкладення електронної пошти, що містить сам вірус, або частина шкідливої програми, яка виконує шкідливі дії. Як тільки жертва відкриває файл, пристрій заражається.

Програми вимагачі- є одним з найбільш прибуткових, а отже, і найпопулярніших видів шкідливих програм серед кіберзлочинців є програми вимагання. Вони встановлюються на комп'ютер жертви, шифрують файли, а потім вимагають викуп (як правило, у біткоїнах) за повернення цих даних користувачеві.

Підроблений антивірус - змушує вас думати, що ваш комп'ютер або смартфон заражені, щоб змусити жертв придбати підроблений додаток. Зазвичай при зараженні підробленим антивірусом під час перегляду веб-сторінок з'являється різні спливаючі повідомлення. Кіберзлочинці використовують ці програми та неетичні методи реклами, щоб залякати користувачів та змусити їх купувати шахрайські програми.

Черви - можуть копіювати себе з комп'ютера на комп'ютер, як правило, за допомогою будь-яких уразливих місць безпеки в програмному забезпеченні чи операційних системах і не вимагають взаємодії користувача ПК для роботи.

Шпигунське програмне забезпечення - це програма, встановлена на комп'ютері, про яку користувач зазвичай не знає і яка отримує доступ та передає

особисту інформацію або модель поведінки користувача. Шпигунське програмне забезпечення дозволяє власникам відстежувати всі форми спілкування на пристрої жертви. Шпигунські програми часто використовуються правоохоронними органами, урядовими установами і організаціями інформаційної безпеки для перевірки та відстеження повідомлень в конфіденційної середовищі або в ході розслідування.

Трояни маскуються під нешкідливі програми, обманюючи користувачів примушують обманом завантажувати та використовувати їх. Після запуску вони можуть викрасти особисту інформацію, спричинити збій пристрою, підглянути ваші дії або навіть здійснити атаку. Але на відміну від інших видів шкідливого програмного забезпечення трояни це саме програми і принцип їх роботи полягає в тому що вони атакують окремий файл і далі або змінюють його або розрушує. Класифікацій у троянів багато але найнебезпечнішими з них є:

а)бекдор, так ще називають віддалений доступ, який надає зловмиснику керування комп’ютером.

б)шпіони, вони відслідковують дії, які робить користувач і надають звіт по цим діям до зловмисника.

в)завантажувачі, цей підвид троянського вірусу працює таким чином, що він завантажує нове і нове шкідливе ПЗ з яким антивірус не змозі справитись.

Рекламні програми - показують користувачам небажану рекламу: зазвичай миготлива реклама або спливаючі вікна з’являються, коли користувач виконує певну дію. Програми часто встановлюються в обмін на іншу послугу, наприклад право користуватися іншою необхідною програмою без оплати повної вартості за неї.

Безфайлове шкідливе програмне забезпечення - це тип шкідливого програмного забезпечення, яке використовує безпечні програми для зараження вашого комп’ютера. Атаки реєстру безфайлового шкідливого програмного забезпечення не залишають шкідливі файли та процеси для сканування та виявлення. Вони не залежать від файлів і не залишають слідів, що може ускладнювати їх виявлення та видалення.

1.4 Оцінка ризиків для систем захисту інформаційних ресурсів

Перш за все, потрібно визначити цінність інформаційних ресурсів. Будь-яка кількісна оцінка ризиків вимагає оцінки вартості інформаційного ресурсу (процесу). Для оцінки цінності інформації слід використовувати теоретичну оцінку, яка розроблена так само добре. Існують такі підходи до оцінок: порівняльний (ринковий), витратний та дохідний. Вибір конкретного підходу за участю визначається інформацією, що підлягає оцінці. Кожен підхід дозволяє підкреслити перші характеристики інформації. Таким чином, при оцінці позицій доходу підходить на перше місце дохід як основний фактор, що визначає високу вартість інформації. Чим більший дохід від інформації, тим більша її ринкова вартість за інших рівних умов. Важливим є тривалість періоду можливого доходу, ступінь та тип ризиків, які здійснюють цей процес.

Дохідний підхід полягає у визначенні теперішньої вартості майбутніх доходів, що виникне в результаті використання майна майбутніх доходів, що виникне в результаті використання інформації та можливого подальшого її продажу.

Порівняльний підхід ефективний у випадку активного ринку порівнянних інформаційних ресурсів. Точність оцінки залежить від якості зібраних даних, використовуючи цей підхід, оцінювач повинен збирати надійну інформацію про останні продажі порівнянних об'єктів. Ефективність цього підходу знижується, якщо операцій було мало, а моменти їх здійснення та оцінки відокремлені довгим періодом, також якщо ринок знаходиться в ненормальному стані, оскільки швидкі зміни на ринку призводять до спотворень. Порівняльний підхід заснований на застосуванні принципу заміщення. Для порівняння відбираються інформаційні ресурси (продукти), що конкурують з оціненою інформацією. Порівняльний підхід базується на принципі заміщення. Для порівняння відбираються інформаційні ресурси інших підприємств, які конкурують з оціненою інформацією. Зазвичай існують відмінності, тому слід коригувати дані.

Витратний підхід до оцінки інформації буде розглядатися як усі витрати, понесені власником інформації на її отримання. Насправді такий підхід є найпростішим для власника інформації, оскільки він знає всі складові витрат. Однак працювати з деякою інформацією може бути не об’єктивно, оскільки одна людина може заробляти більше десяти осіб, які отримують однакову зарплату.

Загалом усі три підходи взаємопов’язані. Кожен з них передбачає використання різних типів інформації. Для кожного підходу важливо враховувати також управління ризиками, тобто вжиття заходів щодо зменшення частоти загроз та зменшення шкоди від них. Залежно від отриманих показників ризику власник інформаційних ресурсів обирає наступні кроки по управлінню та контролю ризиками

До стратегій управління ризиками в сфері інформаційних ресурсів можна віднести такі:

1) Прийняття ризику

Береться до уваги те, що небезпеки для інформаційних ресурсів немає тому вживати конкретних дій для управління не потрібно.

2) Зменшення (зниження) ризику

Ця стратегія обирається коли небезпека існує і необхідне застосування заходів щодо зменшення показника ризику для інформаційних ресурсів;

3) Виключення ризику

Вибір цієї стратегії означає що небезпека реальна і необхідно вжити заходи, що дозволять виключити ризик для власних інформаційних ресурсів;

4) Передача ризику третім особам

Стратегія яка застосовує заходи, що вживаються власником для компенсації можливих наслідків ризику, тобто страхування ресурсів. Обирається задля того щоб мінімізувати для власника втрати.

Таким чином, оцінка та управління ризиками в даний час є методологією, яка найбільш швидко розвивається, оскільки допомагає організаціям оптимізувати ресурси, що виділяються на захист інформації та захищати об'єкти, що знаходяться під найбільшим ризиком. У той же час зрозуміло, чому ризики

природних та техногенних загроз не можна розглядати разом, оцінюючи за тими самими принципами. Природні і техногенні загрози не матимуть такого серйозного впливу на відміну від штучних загроз. Якщо розглядати штучні загрози то для них запропоновано два методи оцінки ймовірного ризику. Перший полягає в тому, що, оцінюючи ризики, ми займаємо позицію зловмисника та оцінюємо ризики зловмисника. Виходячи з цих ризиків, є можливість класифікувати ризики для захищеної організації. Другий прийом полягає у кількісному визначенні ризиків за допомогою системи обмежень, яка відображає адекватність загроз для обраної організації. Тобто за необхідністю визначаються ризики, які пропонується обмежити до того, як вони стануть загрозами для організації.

1.5. Висновки до першого розділу

Підсумовуючи викладене в розділі, можна зробити висновок, що сучасний період характеризується новими взаємовідносинами між обома сторонами інформаційного суспільства - інформаційними ресурсами та інформаційними потребами. Аналізуючи ці дві сторони аналізу можна побачити динаміку та можливий напрям майбутнього розвитку суспільства під час інформаційного вибуху. Отже, можна зробити висновок, що млявий саморозвиток інформаційних ресурсів повинен бути збалансований науково обґрунтованою інформатизацією навчання, спрямованого на інформаційне суспільство та стабільний шлях.

Зростання інформації та її зростаюча роль у всіх аспектах людського життя призвели до величезних інвестицій та зусиль для розвитку інформаційної та комп’ютерної інфраструктури в суспільстві. Наукові дослідження призвели до модернізації техніки цієї галузі, що призвело до такого швидкого зростання інформаційних та обчислювальних можливостей та нового інформаційного циклу інформації, в якому переважна більшість інформації залишається

незатребуваною. Багато інформаційних структур, що пронизують освіту, є єдиною інформаційно-комп'ютерною та науковою інфраструктурою системи освіти, яка сьогодні активно адаптується та розвивається. Швидке зростання комп'ютерних технологій та пізнє розуміння їх теоретичного розуміння в освіті призвели до повсякденного розуміння та використання інформаційних та комп'ютерних систем. Це призвело до спонтанного спотворення інформаційного суспільства, небезпечної однобічності та спотворення ідеї інформатизації комп'ютерних технологій. Крім того, збільшення продуктивності комп'ютерних технологій та поява нових видів атак на системи безпеки знижують стійкість відомих систем, що використовуються для захисту інформаційних ресурсів. Аналіз ризиків, які несуть загрозу для інформаційних ресурсів показав, що найнебезпечнішими загрозами є загрози пов'язані з шкідливим програмним забезпеченням та його дією на ПК. Результатами такої дії може бути як часткова втрата інформації в інформаційному ресурсі так і повне її знищення або блокування чи спотворення. З цієї причини завдання полягає у створенні нової системи захисту, яка враховує нові методи та можливості програмного та апаратного забезпечення для забезпечення більш надійного захисту від шкідливого програмного забезпечення.

РОЗДІЛ 2. ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1 Основні принципи і механізми захисту інформаційних ресурсів

Існує два основних підходи до забезпечення безпеки інформаційних ресурсів:

1)Частковий. Цей підхід зосереджений на протидії строго визначеним загрозам за певних умов (наприклад, спеціалізовані антивірусні засоби, окремі засоби реєстрації та управління, засоби автономного шифрування). Перевагою часткового підходу є висока селективність щодо конкретної загрози. Недоліком є локальність дії, фрагментарні заходи захисту забезпечують ефективний захист конкретних об’єктів від конкретної загрози.

2)Системний. Цей підхід набув широкого поширення через властиві недоліки фрагментарності. Він поєднує різні заходи протидії загрозам і традиційно розглядається як три взаємодоповнюючі сфери. Організація безпечного середовища обробки інформації дозволяє в рамках існуючої політики безпеки забезпечити належний рівень безпеки АІС. Недоліком такого підходу є висока чутливість до помилок при встановленні та конфігурації засобів захисту, складність управління.

Системний підхід до побудови системи захисту з провідною роллю організаційної діяльності. Це означає оптимальне поєднання програмного забезпечення та заходів організаційного захисту, підтверджене практикою створення вітчизняних та іноземних систем захисту. Поділ та мінімізація повноважень щодо доступу до обробленої інформації та процедур обробки. Користувачі отримують тільки ті повноваження, які їм були надані і яких буде достатньо для виконання службових обов’язків пов’язаних зі конфіденційною інформацією. Підхід характеризується повним контролем та реєстрацією спроб несанкціонованого доступу, тобто необхідністю точно встановити особу кожного користувача та записати його дії для можливого розслідування, а також

неможливістю виконання операції з обробки інформації в АІС без реєстрації.

Можна виділити наступні методологічні, організаційні та реалізаційні принципи інформаційної (у тому числі комп’ютерної) безпеки інформаційних ресурсів:

1)Принцип законності. Розроблено в рамках імплементації чинного законодавства про інформаційну безпеку.

2)Принцип невизначеності. Виникає через неоднозначність поведінки суб'єкта, хто, коли, де і що може негативно вплинути на безпеку об'єкта, що охороняється.

3)Принцип неможливості створення ідеальної системи захисту. Він буде базуватися на принципі невизначеності та обмежених ресурсів цих послуг.

4)Принципи мінімального ризику та втрат. Вони виникають через неможливість створення ідеальної системи захисту. У відповідь на це необхідно вивчити конкретні умови існування об’єкта, що охороняється, у кожен момент часу.

5)Принцип безпечного часу. Забезпечує врахування абсолютного часу, тобто протягом якого необхідно тримати об’єкти захисту; та відносний час, тобто тривалість часу з моменту виявлення злочинної діяльності до досягнення зловмисником цілі.

6)Принцип "захисту всіх від усіх". Дозволяє організовувати заходи захисту від усіх форм загроз об'єктам, що охороняються, що є наслідком принципу невизначеності.

7)Принципи особистої відповідальності. Він несе персональну відповідальність для кожного працівника компанії, установи та організації за дотримання режиму безпеки в межах повноважень, функціональних обов'язків та актуальних інструкцій.

8)Принцип обмеження повноважень. Він передбачає обмеження повноважень суб'єкта щодо доступу до інформації, доступ до якої не є необхідним для нормального виконання його функціональних завдань, а також введення заборони на доступ до об'єктів та районів, де перебування не відбувається, вимагається за типом діяльності.

9)Принцип взаємодії та співпраці. Внутрішній прояв передбачає побудову

відносин довіри між працівниками, які відповідають за безпеку (включаючи інформаційну безпеку), та працівниками.

10)Принцип складності та індивідуальності. Він передбачає неможливість забезпечення безпеки об’єкта охорони за допомогою єдиного заходу, але лише за допомогою низки складних, взаємопов’язаних та дублюючих заходів, які проводяться для індивідуальної участі в певних умовах.

Але самих тільки принципів недостатньо, тому що принципи тільки теоретично описують методи та засоби захисту. Разом з принципами впроваджуються наступні механізми безпеки, які більш конкретно описують яким чином можна захистити інформаційних ресурс від тих чи інших видів шкідливого ПЗ.

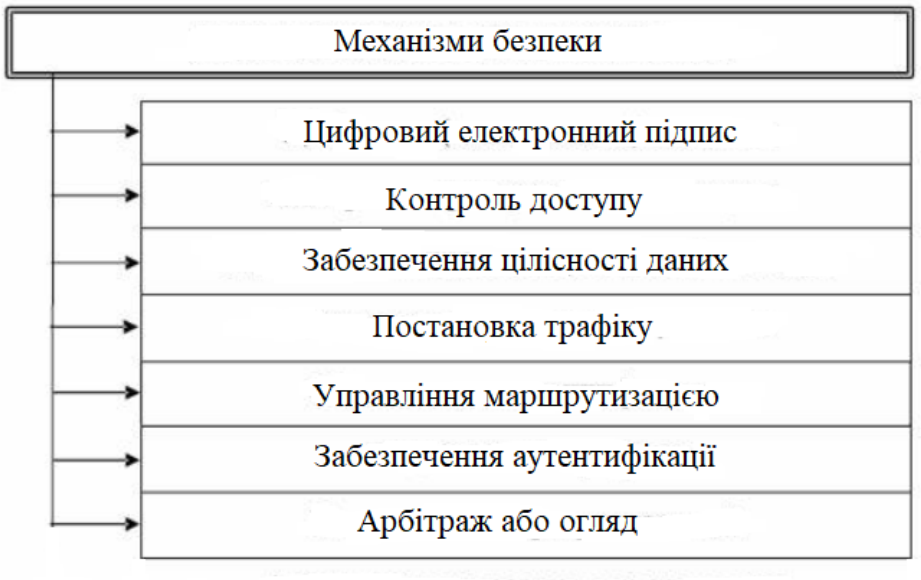

Рис. 2.1 Механізми безпеки інформаційних ресурсів та інформації

Механізми контролю доступу перевіряють авторизацію об'єктів АІС (додатків та користувачів) для доступу до мережевих ресурсів. При доступі до ресурсу за допомогою зв'язку управління здійснюється в точці ініціації, а також у проміжних точках і в кінцевій точці.

Механізми цифрового підпису базуються на асиметричних алгоритмах шифрування і складаються з двох методів створення підпису відправником та його розпізнавання одержувачем:

а) Перший метод передбачає шифрування блоку даних або додавання його

його до криптографічної контрольної суми, і в обох випадках використовується секретний ключ відправника.

б)Другий метод заснований на використанні відкритого ключа, знання якого достатньо для ідентифікації відправника. Але цей метод значно слабший за перший, так як зловмисник може дізнатись відкритий ключ.

Механізми постановки трафіку, які також називають механізмами завершення тексту, використовуються для класифікації потоку даних. Вони засновані на генерації блоків AIC, їх шифруванні та організації передачі через мережеві канали. Це виключає можливість отримання інформації шляхом спостереження зовнішніх властивостей потоків, що циркулюють по каналах зв'язку.

Механізми цілісності даних використовуються або для одного блоку, або для потоку даних. Обов’язковою умовою є цілісність блоку, але це не гарантує цілісність потоку та гарантує реалізацію взаємопов’язаних процесів шифрування та дешифрування відправником та одержувачем. Невідповідність між ними може свідчити про те, що інформація в блоці перекошена та не відповідає дійсності при розшифровці. Однак у принципі описаний механізм не дає можливості виявити заміну одиниці. Щоб цього уникнути, необхідно контролювати цілісність потоку, що реалізується за допомогою шифрування та за допомогою ключів, які змінюються залежно від попередніх блоків.

Механізми управління маршрутизацією забезпечують різноманітні маршрути для переміщення інформації через комунікаційну мережу, щоб запобігти передачі секретної або конфіденційної інформації по небезпечних, фізично ненадійних каналах. Якщо зловмисник знає конкретний спосіб пересилання повідомлення абонента, він може виконати атаку, яка веде до реалізації загрози відмови в обслуговуванні, тобто іншими словами DDoS. Для захисту від таких атак повинні використовуватися спеціальні засоби, які повинні обирати найбільш безпечні та надійні канали зв'язку.

Механізми арбітражу підтверджують властивості даних, переданих третіми сторонами між об'єктами AIC. Для цього вся інформація, надіслана або

отримана об’єктами, передається через так званого «арбітра», завдяки чому він згодом може підтвердити ознаки, згадані вище, тобто відбувається так звана модерація і перевірка відповідності тих даних, якими обмінюються об’єкти автоматизованої інформаційної системи.

2.2 Методи та засоби забезпечення захисту інформаційних ресурсів

Методи інформаційних ресурсів зображені на рисунку 2.2:

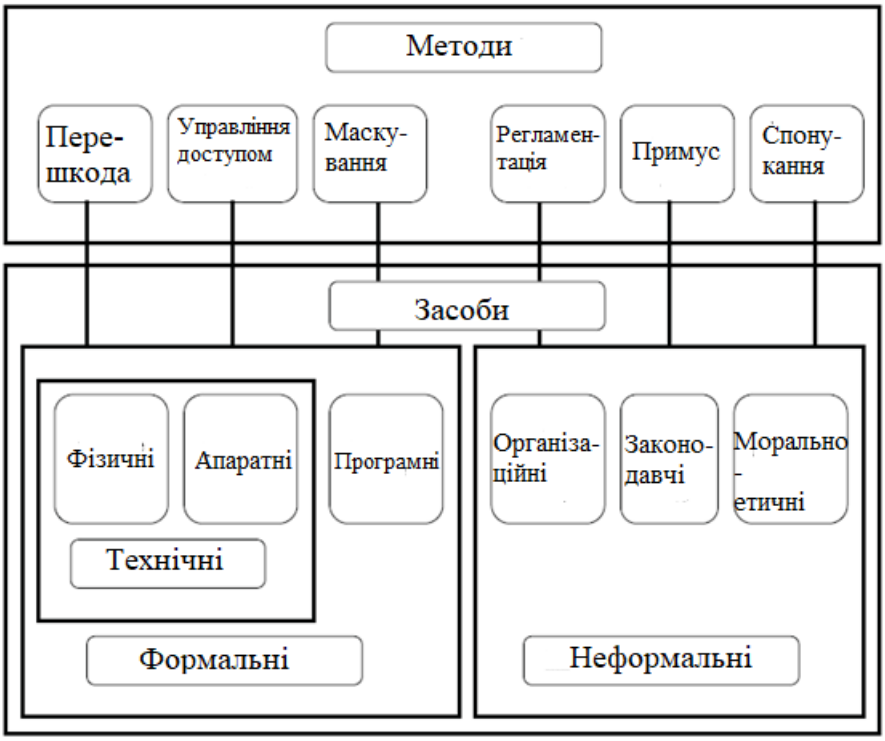

Рис. 2.2. Засоби і методи захисту інформаційних ресурсів.

Перш за все згідно з рисунком є шість методів захисту інформаційних ресурсів:

1)Метод перешкоджання.

Це метод фізичного блокування шляху зловмисника для захисту інформації. Використовується до обладнання або носія інформації які можливо викрасти або навмисно пошкодити.

2)Метод управління доступом

Це захист який застосовує шлях урегулювання і використання всіх ресурсів автоматизованої інформаційної системи підприємства. Контроль доступу який

використовується в методі включає в себе такі функції безпеки:

а)ідентифікація користувачів, персоналу та ресурсів інформаційної системи також присвоєння персонального ідентифікатора кожному об’єкту;

б)автентифікація – це встановлення автентичності об'єкта або суб'єкта за вказаним ним ідентифікатором;

в)перевірка повноважень- це перевірка відповідності дня тижня, часу доби, запрошених ресурсів та процедур встановленими нормами;

г)реагування-це сигналізація, вимкнення, затримка робіт, відмова у запиті на спроби несанкціонованих дій.

3)Метод із застосуванням маскування

Цей метод розроблений на основі захисту інформації в автоматизованій інформаційній системі компанії шляхом її криптографічного блокування.

4)Метод із застосуванням регламентації

Метод створює умови для автоматизованої обробки, зберігання та передачі інформації, що мінімізують можливість несанкціонованого доступу до цієї інформації.

5)Метод із застосуванням примусу

Полягає в тому, що користувачі та персонал системи мають дотримуватися правил щодо оброблення, передавання та використання інформації, при втраті якої буде відповідна матеріальна, адміністративна та кримінальна відповідальність.

6)Метод із застосуванням спонукання

Спонукає користувачів та працівників системи не порушувати встановлені правила та дотримуватися встановлених морально-етичних норм. Ці методи захисту інформації реалізовані з використанням таких матеріальних цінностей як фізичні цінності, апаратно-програмні цінності та криптографічні.

7)Засоби фізичного захисту

Застосовуються для зовнішнього захисту зони об'єктів, захисту компонентів автоматизованої інформаційної системи компанії і які мають вигляд окремої системи, або окремого автономного пристрою.

Щодо апаратних засобів захисту, вони можуть бути як формальні так і не формальні. Формальні в свою чергу поділяються на технічні та програмні, а технічні в свою чергу поділяються на фізичні та апаратні.

1)Апаратні засоби захисту

Це електронні пристрої, які інтегровані безпосередньо в блоки автоматизованої інформаційної системи або спроектовані як самостійні пристрої та підключені до цих блоків. Вони використовуються для внутрішнього захисту конструктивних елементів комп'ютерів і систем. До них можна віднести термінали, також до елементів можна віднести процесори або перефирійні пристрої.

2)Засоби програмного захисту

Виконують функції логічного та інтелектуального захисту і містяться або в програмному забезпеченні автоматизованої інформаційної системи, або в засобах, комплексах та системах пристроїв управління.

3)Програмне забезпечення для інформаційної безпеки є найпоширенішим видом захисту з наступними позитивними характеристиками: універсальність, гнучкість, здатність змінюватися та розвиватися. Цей факт робить їх обох найбільш вразливими елементами захисту корпоративної інформаційної системи.

4)Апаратні та програмні засоби захисту

Це інструменти, в яких програмне забезпечення та апаратне забезпечення повністю взаємопов’язані та нерозривні.

5)Криптографічні засоби

До криптографічних засобів захисту відносяться пристрої, програмні застосунки які для перетворення інформації використовують методи шифрування.

6)Організаційні засоби

Це організаційно-технічні, а також організаційно-правові заходи щодо регулювання поведінки персоналу.

7)Законодавчі засоби

Маються на увазі правові акти країни, які регулюють правила використання, обробки та передачі інформації з обмеженим доступом та встановлюють заходи

відповідальності за порушення цих правил.

За допомогою перерахованих засобів і методів для створення системи захисту можна можна сформувати такі засоби захисту інформаційного ресурсу:

1)Засіб автентифікації і авторизації користувачів.

Основним способом захисту інформації є введення так званих інструментів AAA- автентифікація, авторизація, адміністрування. Інструментами AAA є апаратні та програмні системи ідентифікації та автентифікації (CIA) для комп'ютерів.

При використанні CIA працівник отримує доступ до комп’ютера або корпоративної мережі лише після успішного завершення процедури ідентифікації та автентифікації. Ідентифікацією називають розпізнавання користувача власною або наданою йому ідентифікаційною ознакою. Перевірка належності користувачеві ідентифікаційного знака, представленого йому, здійснюється в процесі автентифікації. Сучасні CIA за типом використовуваних ідентифікаторів поділяються на електронні, біометричні та комбіновані

2)Засіб антивірусного захисту;

Основними вимогами до антивірусного засобу захисту, а саме антивірусу:

а)Стабільність і надійність роботи, тобто її можливість до стабільної роботи і якості її роботи;

б)Наявність великої антивірусної бази з постійним оновлення, тобто актуальні сигнатури вірусів;

в)Ефективна швидкість роботи тобто без затримок та достатньо довгого очікування ;

г)Багатоплатформеність тобто можливість використання на різних платформах, тобто одночасне використання як на серверній частині так і на користувацькій частині.

д)Наявність центральної консолі управління тобто спеціального ПЗ для адміністрування.

е)Евристичний аналіз, тобто перевірка файлу та його вмісту на те, чи присутні в ньому відомі сигнатури вірусів або їх частина.

3)Засіб міжмережевого екранування;

Засіб брандмауера повинна забезпечувати:

а)фільтрація з урахуванням вхідного та вихідного мережевого інтерфейсу як засобу автентифікації мережевих адрес;

б)фільтрація на транспортному рівні запитів на встановлення віртуальних зв’язків з урахуванням транспортних адрес відправника та одержувача;

в)фільтрація на рівні програми запитів до служб додатків з урахуванням адрес заявки відправника та одержувача;

г)фільтрація з урахуванням дати та часу;

д)фільтрація за окремими правилами IP-трафіку локальної віртуальної мережі (зашифрований IP-трафік) та IP-трафіку, який не пов'язаний з обміном даними всередині локальної віртуальної мережі (незашифрований IP-трафік);

4)Засіб криптографічного захисту інформації;

Для криптографічного захисту інформації використовуються засоби криптографічного захисту інформації (ЗКЗІ), тобто це можуть бути як апаратні, програмні так і апаратно-програмні засоби, які для захисту використовують алгоритми криптографічної зміни інформації та які використовуються для захисту інформації коли вона передається та (або) для захисту інформації від несанкціонованого доступу під час її оброблення та зберігання.

5)Засіб захисту WEB-серверу.

Засіб захисту WEB-серверу складається з програмної реалізації коду, який буде захисту WEB-серверу від шкідливого програмного забезпечення, а саме атак типу DDoS.

6)Засіб фізичного захисту;

Засіб фізичного захисту інформації використовується для протидії навмисним загрозам впливу зловмисника і стихійним силам, насамперед пожежам. Засоби реалізують методи фізичного захисту за допомогою інженерних конструкцій і технічних засобів охорони. Необхідність і ефективність інженерного захисту та технічної охорони об'єктів підтверджується статистикою, відповідно до якої більше 50% вторгнень відбувається на

комерційні об'єкти з вільним доступом персоналу та клієнтів і тільки 5% - на об'єкти з посиленим режимом охорони, із застосуванням спеціально навченого персоналу і складних технічних систем охорони.

7)Засіб резервного копіювання та архівування.

Одним із ефективних методів боротьби з наслідками модифікації та втрати інформації а також атак на інформаційні ресурси за допомогою шкідливого програмного забезпечення, модифікацією та втратою інформації через є правильна організація резервного копіювання даних. Цей засіб відповідає за створення резервних копій:

1) жорстких дисків та їх розділів з усіма даними, що зберігаються на них, операційні систем та додатків;

2) найважливіших для користувача файлів та папок.

2.3 Висновки до другого розділу

Аналіз досвіду в країні та за кордоном переконливо свідчить про необхідність створення комплексної системи захисту інформації, яка координує оперативні, оперативні, технічні та організаційні захисні заходи. Система безпеки повинна бути оптимальною для використання методів та інструментів, а також для механізмів захисту інформаційних ресурсів. Слід також враховувати взаємозв'язок між якістю та вартістю захищених ресурсів. Потрібна гнучкість та адаптація системи до швидкозмінних факторів середовища, організаційного та соціального середовища на об'єкті. Досягнення такого рівня безпеки неможливе без використання системного підходу до захисту інформаційних ресурсів та розробки політики інформаційної безпеки в компанії. На основі цих даних були створені апаратні, фізичні, та програмні засоби для захисту інформаційних ресурсів, які необхідно впровадити для захисту від шкідливого програмного забезпечення.

РОЗДІЛ 3. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

3.1 Опис фізичних, апаратних та програмних засобів системи захисту інформаційних ресурсів

Структурна схема системи захисту виглядає наступним чином:

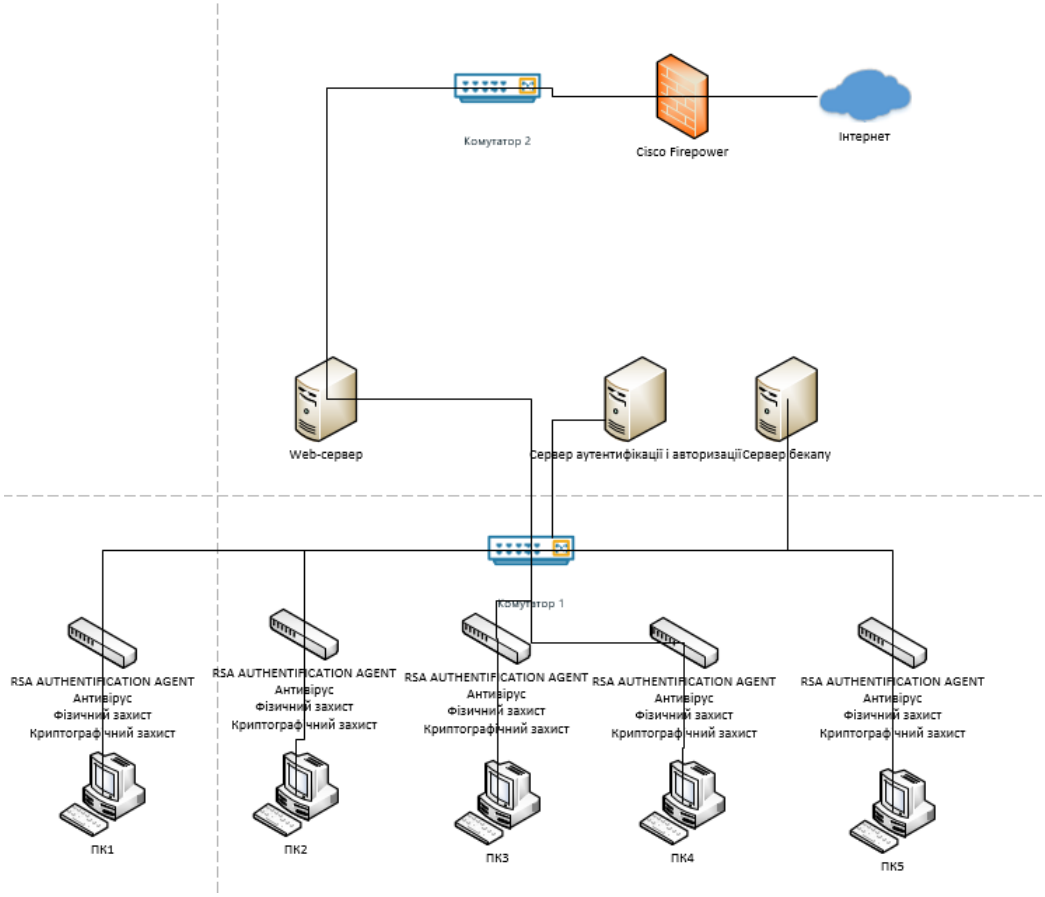

Рис.3.1 Структурна схема системи.

Структурна схема системи захисту інформаційного ресурсу від шкідливого програмного забезпечення складається з семи засобів і використовує лише ліцензійне програмне забезпечення:

1) Засіб автентифікації і авторизації користувачів.

Засіб автентифікації та авторизації є критично важливим, він обмежує доступ користувачів, ідентифікація та автентифікація повинні бути не тільки в

системах безпеки, але і при створенні будь-якої інформаційної системи. В даний час інформаційно-комунікаційний простір розвивається надзвичайними темпами, системи та послуги стають все більш розподіленими; водночас зростає роль правильного вирішення проблеми надання доступу. У той же час, у зв'язку з масовою інформатизацією та розвитком технологій, до систем доступу пред'являються дедалі жорсткіші вимоги щодо захисту від дій зловмисників, як зовнішніх, так і внутрішніх. Одночасно зростає роль надійної ідентифікації користувачів та ресурсів, оскільки сучасні методи автентифікації дозволяють персоналізувати дії користувачів, а системи контролю доступу - з достатнім ступенем надійності використовуються для захисту інформаційних ресурсів від дій зловмисників.

Існують такі комплекси автентифікації і авторизації користувачів: Fido, Sidway, Рутокен, Google authenticator та RSA SecurID. RSA SecurID серед цих комплексів є найкращим при співвідношенні принцип роботи/якість є RSA SecurID так інші не мають окремого програмного забезпечення як для серверу для фіксації дії так і для ПК. Google authenticator працює по принципу з’єднання з інтернетом а для забезпечення вищого рівня безпеки необхідне ПЗ яке буде автономне та працюватиме без підключення до інтернету.

2)Антивірусний засіб.

Антивірусний засіб створений для забезпечення безпеки інформаційних ресурсів, тобто це програмно-апаратний засіб, тобто єдиний комплекс для створення надійного антивірусного захисту інформаційної бази, що знаходиться в локальній мережі. Комплексний підхід до використання засобу полягає в організації управління будь-якими потоками інформації, що протікають в захищеній локальній мережі. Для ефективної роботи системи, що забезпечує надійний захист від шкідливого впливу вірусів усіх елементів інфраструктури, необхідний високий рівень узгодженості між методами та інструментами.

Аналізуючи ринок популярних антивірусних засобів можна виділити такі популярні антивіруси: Avast, Kaspersky, Dr.Web, Avira, ESET, AVG, Comodo, Symantec та інші.

Порівняння антивірусних засобів зображено на рисунку 3.2.

Рис.3.2 Антивірусні засоби захисту.

Для порівняння візьмемо такі параметри як кількість знайдених загроз, відсоток знайдених загроз, завантаження центрального процесору і час на пошук загроз.

Таблиця 3.1

Антивірус/ Характеристика	Кількість знайдених загроз	Завантаження центрального процесору	Час на пошук загроз	Відсоток знайдених загроз
Dr.Web	3695	80-90%	23-25 хв	94%
Avast	2107	40-50%	10 хв.	81%
AVG	2840	15-30%	9-10 хв.	84%
Касперський	3489	60-80%	20 хв	91%
Comodo	2255	45-55%	7-10 хв.	57%
Symantec	2497	40-50%	8-10 хв.	54%
ESET NOD32	1949	40-50%	5-7 хв.	50%

Провівши дослідження перевагою Dr.Web над іншими є спрощене управління робочими станціями антивірусної мережі за допомогою механізму групи, швидке та ефективне розповсюдження оновлень бази даних вірусів та

модулів програм на захищених робочих станціях сервером Dr.Web Enterprise Security Suite, мінімізація мережевого трафіку локальних мереж, побудованих на основі протоколів TCP / IP, IPX, за допомогою використання спеціальних алгоритмів стиснення, ізоляція заражених об’єктів у карантин, а не видалення одразу, вибір типу об'єктів, що підлягають скануванню, можливість оптимізації сканування трафіку за допомогою технології Preview. Також аналізуючи тест, можна сказати що Dr.Web доцільніше обрати як антивірусний засіб для системи захисту.

3) Засіб міжмережевого екранування.

Як правило, брандмауери захищають внутрішню мережу підприємства від проникнення глобальної мережі Інтернет, хоча їх також можна використовувати для захисту від атак корпоративної інтрамережі, до якої підключена локальна мережа.

Для вибору апаратного брандмауеру необхідно порівняти брандмауери які зараз існують на ринку для цього використаємо таблицю 3.2:

Таблиця 3.2

Брандмауери	**Cisco ASA 5515 -X**	**Juniper SRX 220**	**Checkpoint 4210**
Пропускна спроможність Мб/сек	1200	950	1300
Пропускна спроможність з використанням IPS	400	100	1150
Підключень в секунду	15000	-	1000
VPN-трафік	250	100	210

Проаналізувавши такі характеристики як пропускна спроможність, пропускна спроможність з використанням IPS, кількість підключень в секунду та VPN-трафік, можна зробити висновок, що оптимальним варіантом для апаратного міжмережевого екрану є модель брандмауера Cisco ASA 5515 –X. Також на ПК користувачів пропонується використання вбудованого програмного міжмережевого екрану Windows і налаштувати його за необхідністю.

4)Засіб криптографічного захисту інформації.

Це засоби криптографічного захисту інформації які забезпечують цілісність, конфіденційність, достовірність критичної інформації, а також забезпечують юридичне значення електронних документів в ІБ. За цілою низкою функцій засіб співпрацює з засобом авторизації та автентифікації. Засіб криптографічного захисту з точки зору управління ключами підтримується підсистемою управління ISS.

Серед засобів криптографічного захисту інформації можна виділити такі криптографічні програми BestCrypt Volume Encryption, Windows BitLocker та Knox. Windows BitLocker на відміну від двох інших не має шифрування динамічних дисків та ціна за ліцензію завищена, Knox розроблена під ОС Mac і не може працювати з ОС Windows тому найкращим варіантом є BestCrypt Volume Encryption.

5) Програмний засіб захисту WEB-ресурсу.

Засіб використовує мову програмування Lua, що використовується для написання скриптів. Швидкість виконання хорошого коду Lua дещо поступається швидкості хорошого коду C. Але розробка в Lua відбувається швидше і простіше, і сценарії можна змінювати без перекомпіляції сервера. При наступному перезавантаженні вони будуть прочитані, скомпільовані LuaJIT, і це все, що потрібно.

6) Засіб фізичного захисту.

Основу засобів інженерного захисту та технічного захисту об'єктів складають механічні засоби та інженерні споруди, що перешкоджають

фізичному переміщенню зловмисників до місця розташування об'єктів захисту, технічні засоби, що інформують персонал охорони про проникнення зловмисників у контрольовану зону та дозволяючи спостерігати за ситуацією в них.

Проникнення зловмисників може бути прихованим, з механічним руйнуванням інженерних споруд та охоронного обладнання за допомогою інструменту чи вибуху, а в рідкісних випадках у формі збройного нападу з нейтралізацією охорони.

Для засобу фізичного захисту необхідна простота в використанні та обслуговуванні, тому доцільно використати портативний сканер з біометричним методом ідентифікації для захисту робочих станцій. На ринку представлені такі портативні сканери з біометричним методом ідентифікації(таблиця 3.3):

Таблиця 3.3

	BioLink U-Match 3.5	Secugen Hamster Pro	BioLink U-Match BI
Розширення	508	500	508
Час розпізнавання	1/15 сек.	0,02-0,05 сек.	1/15 сек.
Шанс на помилку	10^{-9}	10^{-9}	10^{-9}
Підтримка Win 10	-	+	+

Аналізуючи такі параметри як розширення сканеру, тобто кількість пікселів на дюйм, час розпізнавання , шанс на помилку та підтримку актуальної версії ОС Windows, можна зробити висновок, що всі сканери мають однаковий шанс на помилку, тобто 1 помилка на 1 млн випадків, час розпізнавання найкращий має біометричний зчитувач Secugen Hamster Pro, також він має

підтримку актуальної ОС Windows, тому саме його доцільно використати для системи.

7)Засіб резервного копіювання та архівування

Одним з ефективних методів боротьби з наслідками інформаційних та комп'ютерних катаклізмів, модифікації та втрати інформації є правильна організація резервного копіювання даних в системі захисту інформаційних ресурсів.

До програмних засобів резервного копіювання та архівування можна віднести такі застосунки: Acronis True Image, Déjà Dup, Zinstall Backup, Areca Backup. Zinstall Backup(таблиця 3.4).

Таблиця 3.4

	Acronis True Image	**Zinstall Backup**	**Areca Backup**	**Déjà Dup**
Відкритий код	-	-	+	+
Відновлення втрачених даних	+	+	-	+
Клонування дисків	+	-	+	-
Графік створення резервних копій	+	-	-	-

Аналізуючі застосунки можна зробити висновок, що Areca Backup і Déjà Dup мають відкритий код тому це робить їх уразливими, так як зловмисник може використати це щоб проникнути до інформаційного ресурсу. Zinstall Backup на

відміну не має стільки фунціоналу як Acronis True Image, а саме відновлення втрачених даних, додаткові резервні копії, графік створення резервних копій, клонування дисків, диференційні резервні копії. Тому Acronis True Image доцільно використати для системи захисту інформаційного ресурсу від шкідливого програмного забезпечення.

3.2 Дослідження системи захисту

1) Засіб автентифікації та авторизації

Для реалізації засобу автентифікації і авторизації користувачів, доцільно використати методи двофакторної автентифікації на основі технології RSA SECURID щоб мінімізувати ризик несанкціонованого доступу до ПК.

Ця технологія включає 3 компоненти:

Менеджер автентифікації RSA(RSA Authentication Manager) - це серверна частина. Встановлюється на окремому комп’ютері. Зберігає базу користувачів, журнал подій. Обробляє інформацію, надіслану агентами.

Агенти автентифікації RSA(RSA Authentication Agents) - це агенти. Встановлюється на ресурсах, які потрібно захистити. Замінює запит на введення логіна та пароля, на запит відповідної інформацію SecurID (логін+пін-код+токен-код), далі це перевіряється за допомогою центрального сервера та, на основі цієї перевірки, надається доступ або забороняється доступ.

Апаратні та програмні засоби автентифікації (Hardware&Software Authenticators) - токени та програмне забезпечення, що їх замінює. Розташовані безпосередньо у користувача, вони відображають поточне значення одноразового пароля.

RSA Authentication Manager

Це програмне забезпечення встановлюється на окремому комп'ютері. Виконує наступні завдання:

-зберігає базу користувачів;

-веде журнал подій;

-веде список зареєстрованих токенів;

-обробляє інформацію, надіслану агентами.

Один сервер може обробляти запити десятків агентів. Крім того, є можливість побудувати систему з декількох серверів таким чином, що кожен сервер захищає свою зону, і одночасно може взяти на себе обробку запитів у разі відмови одного з серверів. Базова ліцензія надає один центральний сервер і одну репліку, розширена ліцензія - дев'ять реплік. Підтримуються такі операційні системи: Microsoft Windows Server, Sun Solaris, Red Hat Linux, SuSE Linux Enterprise Server, HP-UX, IBM AIX.

RSA Authentication Agents

Це програмне забезпечення має бути інстальовано на ПК. Основне завдання - вимагати від користувача ввести інформацію SecurID, надсилати її на центральний сервер і, залежно від відповіді, надати доступ або заборонити доступ. Список ресурсів, які можна захистити, величезний. Він включає веб-сервери, мережеві ресурси, сервери VPN та комутований доступ, поштові сервери, робочі станції, віддалені сервери додатків.

Hardware&Software Authenticators

Цей компонент системи SecurID виконується у вигляді брелока для ключів або програмного забезпечення, відображає поточне значення коду токена і завжди знаходиться у користувача, який має певний ідентифікатор. На сьогоднішній день існує велика різноманітність типів електронних токенів. Кожен токен має вбудований акумулятор, якого вистачає на все життя цього токену, тобто від двох до п’яти років, в залежності від типу цього токена. Під час роботи пристрій не потребує ніякого технічного обслуговування та заміни акумулятора. Принцип роботи токену полягає у наступному кожному токену відповідає 128-бітне випадкове число – це називається вектором початкової генерації, також у кожен токен вбудований годинник. Код токена є результатом запатентованого RSA алгоритму, який приймає в якості параметрів поточний час та вектор початкової генерації. У цьому випадку алгоритм працює в одному

напрямку, тому відновити початковий вектор генерації з коду токена неможливо. Код токена змінюється раз на хвилину, його час дії також складає одну хвилину і лише один раз. Через хвилину буде створений новий токен. Оскільки сервер зберігає вектори початкового покоління, що відповідають токенам, він може відновити поточний код токена в будь-який час, використовуючи той самий алгоритм. Якщо годинник сервера та годинник токена розходяться, забезпечується автоматична синхронізація. Принцип синхронізації сервера та токена на рисунку 3.3.

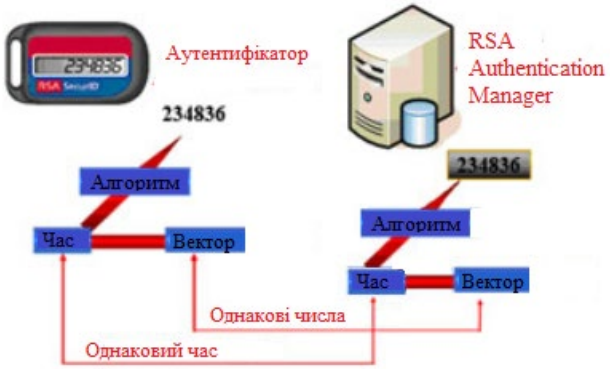

Рис. 3.3.Принцип роботи RSA Authentication Manager та токену.

Прикладами токенів є:

Токен в формі брелока для ключів RSA SecurID SID700.

Рис. 3.4. Токен RSA SecurID SID700.

Токен RSA SecurID SD200.

За формою аналогічний банківської пластиковій картці. Виконаний з металу, його товщина близько 5 мм.

Рис. 3.5 Токен RSA SecurID SD200.

Токен RSA SecurID SD520.

За розмірами аналогічний як SD200, але також цифрову панель. Користувач набирає пін-код на цій панелі і як результат токен відображає не просто токен-код, а комбінацію пін-коду і токен-коду, яка вводиться при автентифікації. Таким чином забезпечується збереження пін-коду, навіть якщо записуються натискання клавіш. Токен RSA SecurID SD520 зображений на рисунку 3.6.

Рис. 3.6 Токен RSA SecurID SD520.

Процедура налаштування RSA Authentication Manager та RSA Authentication Agent.

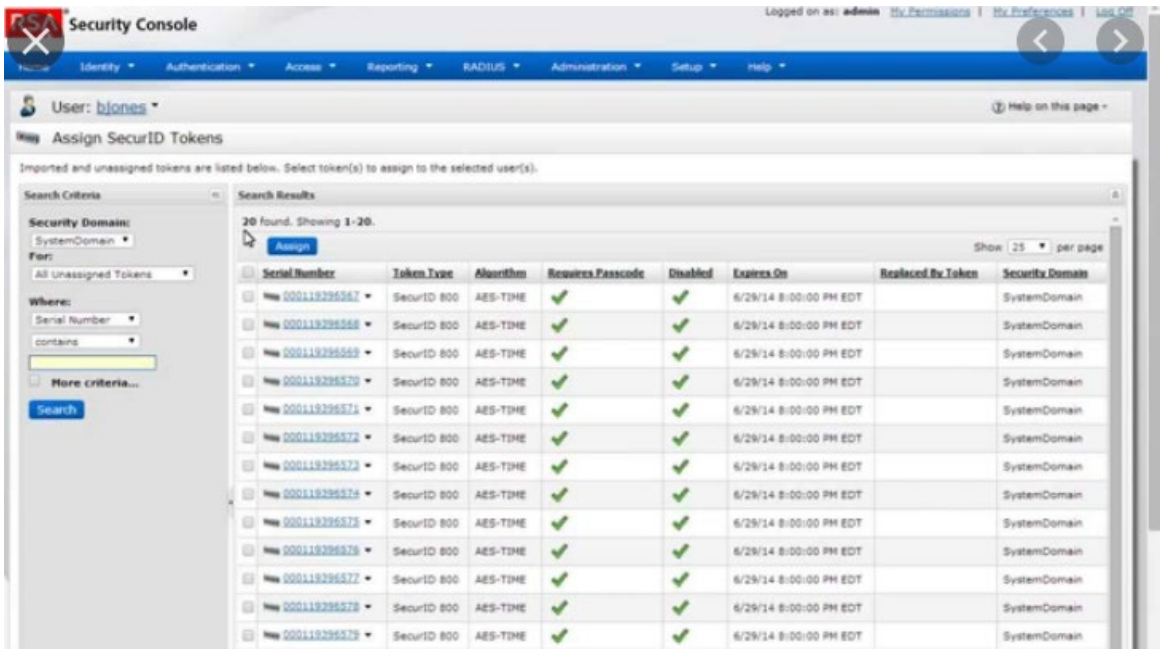

Рис. 3.7. Консоль управління RSA Authentication Manager.

1. В консолі безпеки необхідно натиснути «Доступ» далі «Агенти автентифікації» далі «Додати нового».

2. У меню «Домен безпеки» необхідно додати домен безпеки, до якого потрібно додати нового агента.

3. У розділі «Основи агента автентифікації» необхідно виконати такі дії:

3.1. Для «Ім'я хосту» ввести нове ім’я хосту для хосту агента, а потім клацнути «Визначити IP». IP-адреса вводиться автоматично. Якщо вводити нове ім'я, воно має бути унікальним.

3.2. (Необов’язково) У полі «IP-адреса» ввести IP-адресу агента.

Якщо використовувати існуюче ім'я сервера, це поле автоматично заповнюється і доступне лише для читання. Якщо адреса не вказана, агенти UDP використовуватимуть автоматичну реєстрацію для надання адреси серверу.

3.3. (Необов’язково) У полі «Альтернативні IP-адреси» введіть альтернативні IP-адреси агента.

Це необхідно, якщо агент має більше однієї картки мережевого інтерфейсу або знаходиться за брандмауером мережевих адрес. Якщо використовується існуюче ім'я сервера, це поле автоматично заповнюється та доступне лише для читання.

4. (Необов’язково) У розділі «Атрибути агента автентифікації» можна вибрати такі параметри:

• Вказати тип агента.

Якщо агент є веб-агентом, необхідно обрати «Веб-агент», або зберегти стандартний вибір «Стандартний агент». Типи заповнених агентів є мітками для RSA Authentication Manager, але функціональної різниці при виборі веб-агента або стандартного агента немає. Щоб вимкнути агента, необхідно обрати «Агент вимкнено». Цей параметр створений щоб тимчасово припинити доступ до ресурсу.

• Щоб додати обмеженого агента, необхідно обрати «Дозволити доступ лише для користувачів групи» яким надано доступ до цього агента.

• Щоб призначити новому агенту ручний або автоматичний список контактів,

можна використати «Кнопки списку контактів менеджера автентифікації».

5. (Необов'язково) Щоб налаштувати спосіб автентифікації користувачів із довіреної області до цього агента, необхідно обрати «Увімкнути надійну автентифікацію сфери», а потім обрати, чи дозволити всім довіреним користувачам проходити автентифікацію через нового агента або лише тим надійним користувачам, які належать до групи надійних користувачів, якій надано явний дозвіл на використання агента.

7. Останнім кроком є вибір пункта «Зберегти»

Після цього користувачеві надається фізичний токен який він використовує для входу в систему.

2)Засіб антивірусного захисту

Для реалізації антивірусного засобу захисту використовується програмний продукт Dr.Web Office Shield:

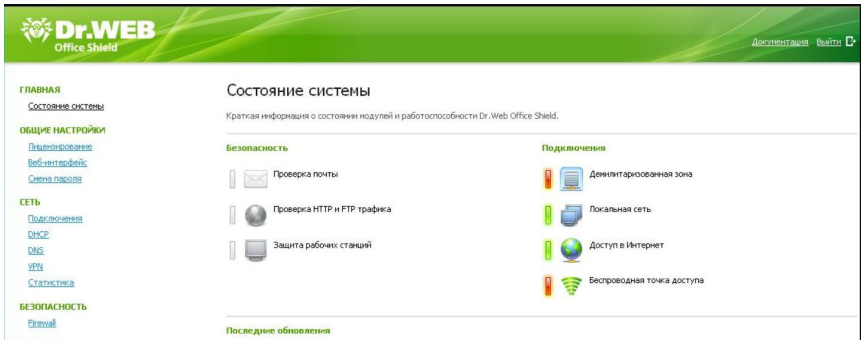

Рис. 3.8 Інтерфейс програмного продукту Dr.Web Office Shield.

Для управління Dr.Web Office Shield достатньо базових знань комп'ютера. Завдяки інтуїтивно зрозумілому інтерфейсу процес адміністрування пристрою простий і може здійснюватися за допомогою будь-якого Інтернет-браузера. Крім того, адміністрування здійснюється за допомогою звичайної консолі, встановленої на робочій станції адміністратора, або через термінал SSH, що дозволяє точно налаштувати пристрій. Висока стабільність, попередньо налаштована конфігурація, автоматична діагностика та запобіжні функції мінімізують необхідність активного адміністративного контролю за роботою Dr.Web Office Shield.

Процедура налаштування:

Встановлення та введення в експлуатацію Dr.Web Office Shield складається з декількох простих кроків. У більшості випадків потрібно лише налаштувати його для конкретних параметрів локальної мережі, і засіб буде виконувати всі покладені на нього завдання. Це стало можливим завдяки використанню оптимізованого програмного забезпечення для операційних систем та зручної системи управління та конфігурації для адміністратора, використання вже встановленого антивірусного сценарію безпеки.

1.Для початку потрібно:

• Зареєструвати продукт за ліцензією.

• Змінити пароль за замовчуванням.

• Перевірити та встановити (якщо потрібно) системний час.

• Перевірити наявність оновлень.

2. Переглянути стан системи

• Виконується на головній сторінці стану системи.

3. Налаштування DNS-серверу або DHCP-серверу

• За замовчуванням DNS-сервер, що входить до складу Dr.Web Office Shield, вимкнено.

• DNS увімкнено та налаштовано на сторінці Network DNS.

Так як антивірусний засіб використовується як внутрішній антивірусний сервер захисту, то необхідно увімкнути та виконати стандартне налаштування DNS-серверу

4. Налаштування мережевих та Wi-Fi з'єднань

Так як антивірусний засіб використовується як внутрішній антивірусний сервер захисту, необіхідно заборонити використання з’єднання WAN та налаштувати параметри підключення до локальної мережі.

6. Налаштування компонентів захисту

• Параметри брандмауера керуються на сторінці безпеки брандмауера.

• Є можливість ввімкнути та налаштувати веб-проксі на сторінці захисту веб-проксі.

• Поштовий проксі ввімкнено та налаштовується на сторінці «Захист поштового

проксі».

7. Оновлення програмного забезпечення Dr.Web Office Shield

• Наявність та доступність нових оновлень відображається як повідомлення у верхній частині будь-якої сторінки системи;

• Примусова перевірка наявних оновлень та встановлення доступних оновлень виконується на сторінці «Оновлення системного програмного забезпечення».

10. Відновлення Dr.Web Office Shield у разі системних проблем

Збереження та відновлення здійснюється на сторінці «Збереження та відновлення системи.»

3)Засіб міжмережевого екранування

Засобом міжмережевого екранування буде Cisco ASA 5515-X для системи та Windows Firewall для ПК користувачів.

Процедура налаштування Cisco ASA 5515-X:

Для конфігурації інтерфейсу і IP-адреси необхідно в консолі Cisco ASA 5515-X використати такі команди:

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

Рис.3.9 Конфігурація та налаштування інтерфейсу і IP-адреси.

Також в налаштуваннях брандмауера необхідно виконати налаштування WEB-серверу за допомогою таких команд:

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

Рис. 3.10 Налаштування WEB-серверу в консолі управління брандмауера.

Процедура налаштування Windows Firewall

1)Необхідно клацнути на іконку пошуку поруч із пунктом «Пуск» і ввести фразу «Панель управління».

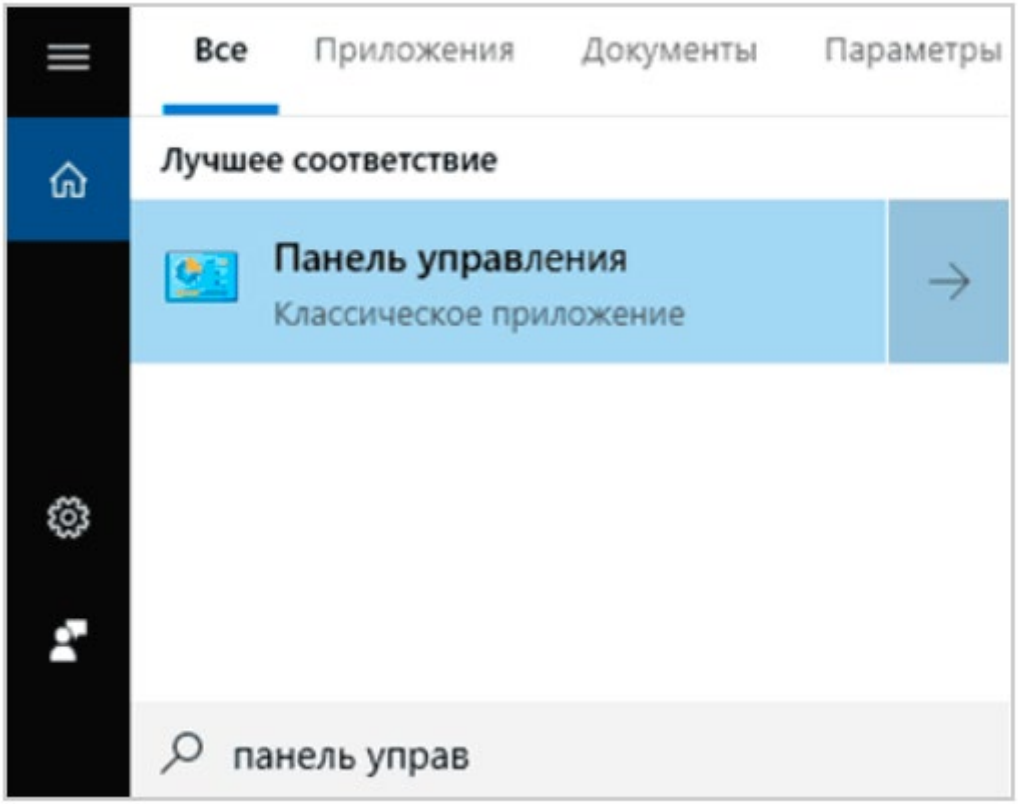

Рис. 3.11 Пошук налаштування «Панель управління»

2) В наступному вікні серед вибору всіх параметрів, які має операційна система Windows 10, необхідно перейти до такого параметру як «Брандмауер захисника Windows». Брандмауер Windows має вбудований протокол безпеки, який збирає IP-адреси та інші дані, пов’язані з підключеннями в домашніх та офісних мережах або в Інтернеті. Тобто є можливість записувати як успішні з’єднання, так і пропущені пакети. Таким чином, ви можете відстежувати, коли комп’ютер у мережі підключається, наприклад, до веб-сайту.

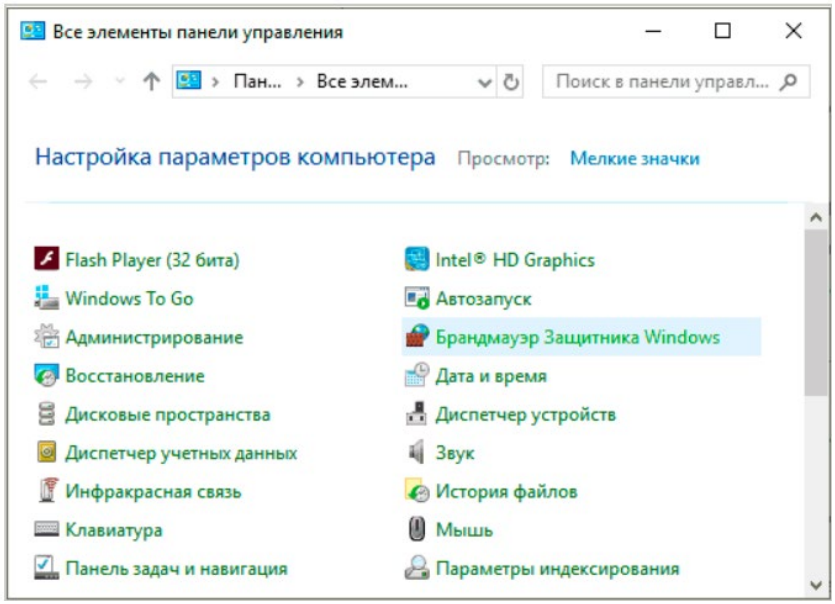

Рис. 3.12 Вибір пункту «Брандмауер захисника Windows»

3) У наступному вікні обираємо пункт «Додаткові параметри», щоб відкрити додаткові можливості налаштування брандмауера.

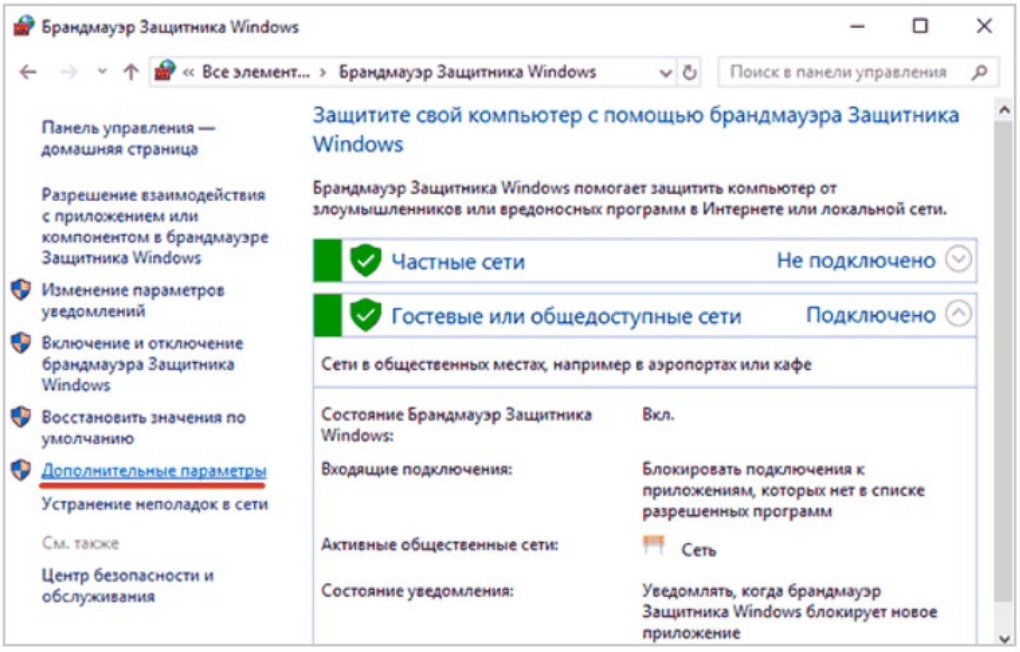

Рис. 3.13 Пункт меню «Додаткові параметри».

4) Перебуваючи в меню «Додаткові параметри», можна побачити поточний стан захисника та його основні налаштування. Ця інформація знаходиться в першому пункті "Монітор брандмауера". До нього відноситься правила для вхідного трафіку та правила для трафіку, який виходить, також входять правила безпеки та правила спостереження.

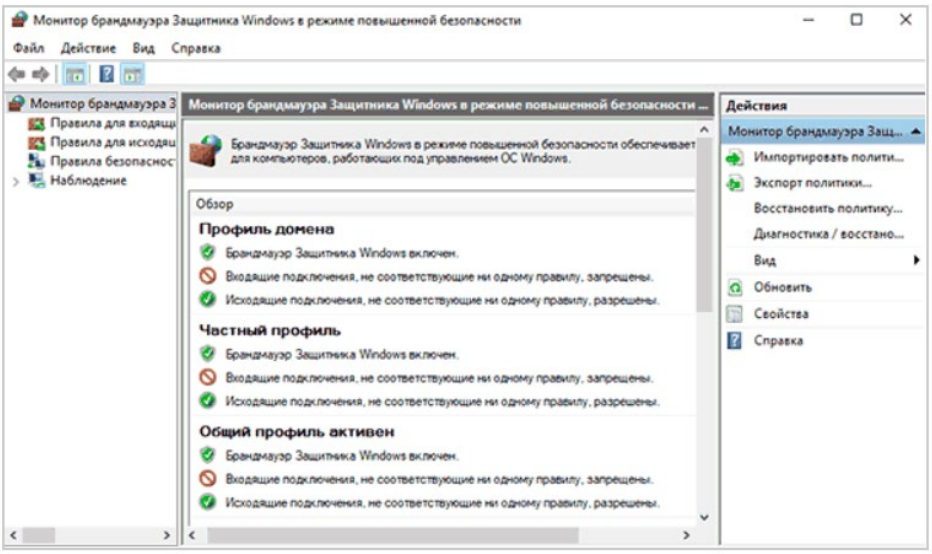

Рис. 3.14 Пункт меню "Монітор брандмауера"

Щоб створити власне блокування певних програм, слід скористатися стовпцем "Правила для вихідних з'єднань", де слід вибрати пункт "Створити правило".

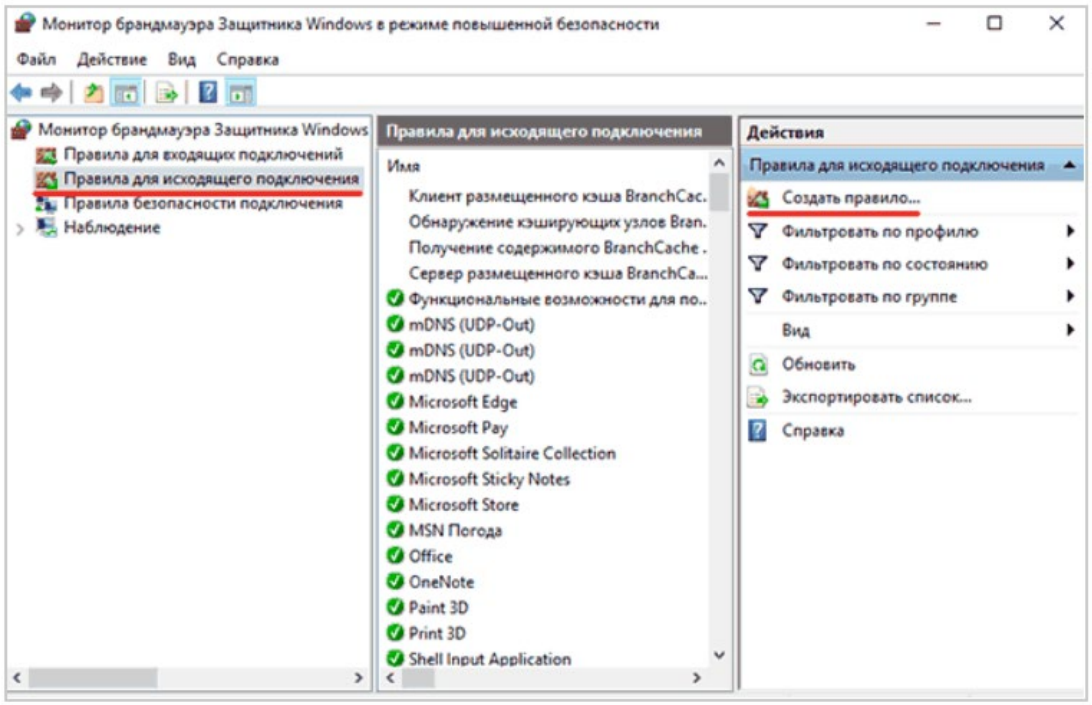

Рис. 3.15 Пункт "Створити правило".

5)У вікні, що відкриється, є кілька варіантів блокування мережі, а саме блокування певної програми, блокування обраного порту, правило яке керує підключеннями для операцій операційної системи Windows та правило, яке користувач може власноруч налаштувати в залежності від того, що йому необхідно. Для системи буде використано блокування необхідної програми.

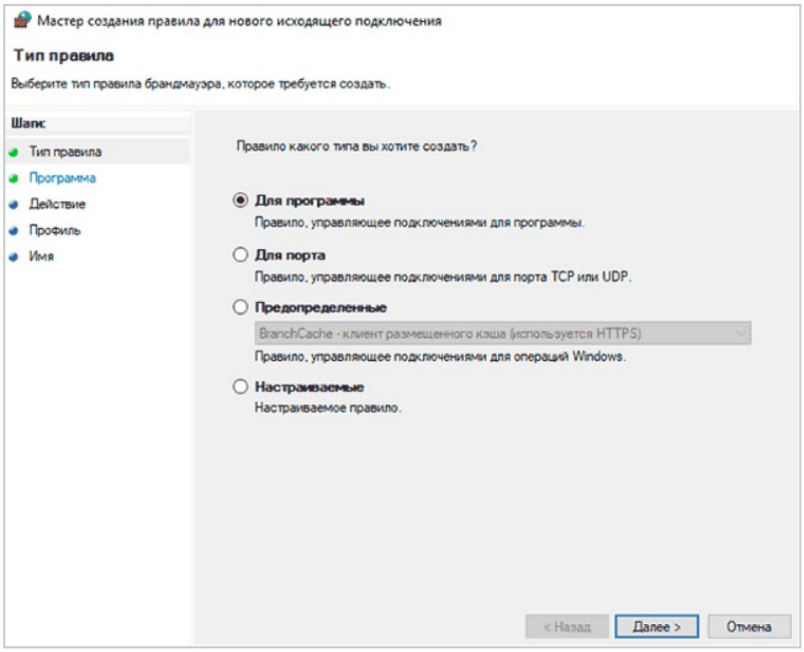

Рис. 3.16 Варіанти блокування мережі

6)Щоб заблокувати певну програму, необхідно обрати пункт «Шлях програми» та вибрати необхідну програму. Наприклад, блокування буде здійснено браузера Google Chrome. Файл браузера знаходиться у шляху "C: \ Program Files (x86) \ Google \ Chrome \ Application".

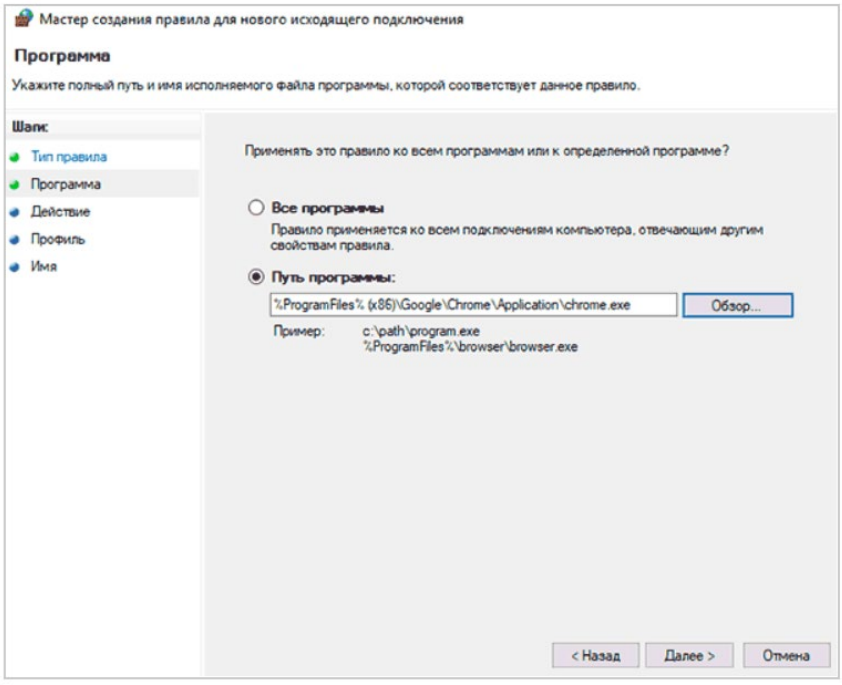

Рис. 3.17 Блокування браузера Google Chrome.

7) Вибравши необхідну програму, слід вибрати дію, яка буде застосована. Щоб заблокувати, необхідно обрати пункт «Заблокувати з’єднання», а потім «Далі».

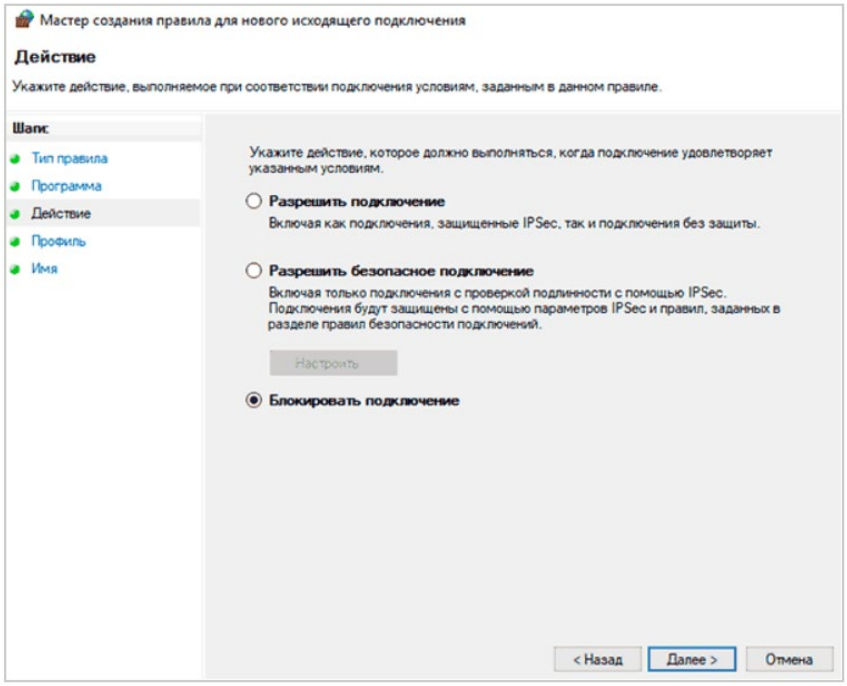

Рис. 3.18 Блокування з’єднання для програми.

8) У наступному вікні обираються профілі, до яких буде застосовано створене правило блокування. Це показано на рис. 3.17.

Серед варіантів є профілі домену, це використовується при підключенні до домену організації, також варіантами профілю є приватний та публічний, до приватного відносяться власні мережі, вдома або на роботі, а до публічного мережі загального користування.

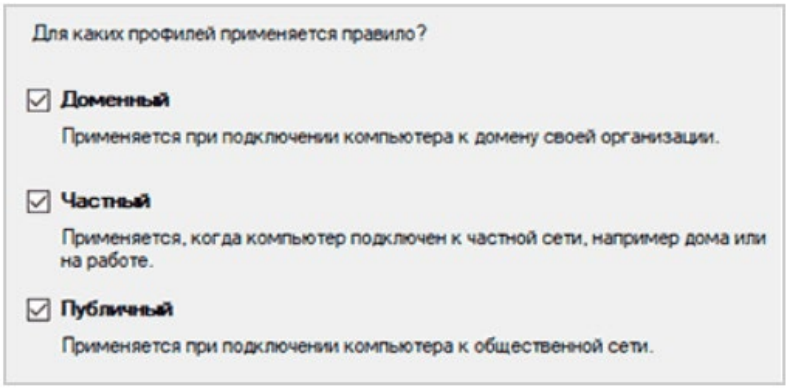

Рис.3.19 Профілі до яких буде застосовано створене правило блокування.

9) В останньому вікні потрібно вказати назву правила для якого створюється виключення. Також є поле «Опис» яке можна використати для написання необхідних користувачу нотаток. Для підтвердження дії треба скористатися кнопкою «Готово».

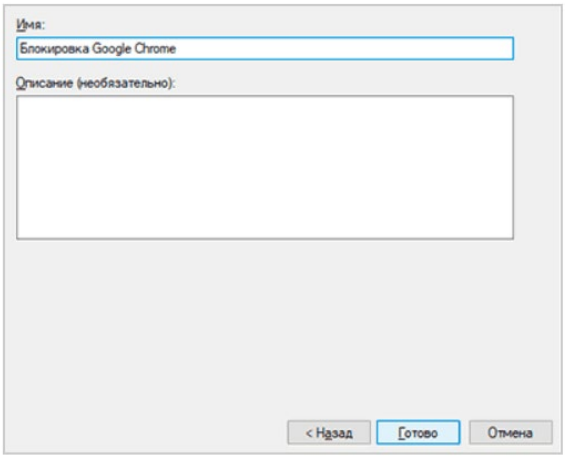

Рис. 3.20 Підтвердження створення правила на блокування.

Таким самим чином можна заблокувати обраний порт.

4)Засіб криптографічного захисту

Засобом криптографічного захисту було обрано програму BestCrypt Volume Encryption. Утиліта BestCrypt Volume Encryption може шифрувати не тільки окремі розділи жорстких дисків або мобільних дисків, таких як флеш-накопичувачі, але й різні розподілені томи: прості охоплені томи, дзеркальні томи та томи RAID5. Ця функція дозволяє використовувати розглянуту програму для захисту комерційних даних, розміщених на серверах.

Особливістю BestCrypt Volume Encryption є велика кількість криптографічних технологій, реалізованих у ньому. Цей продукт використовує такі алгоритми для захисту своєї інформації: AES (256 біт довжина ключа), Blowfish (448 біт), CAST (128 біт), RC6 (256 біт), Serpent (256 біт), Twofish (256 біт). Усі вони вважаються надійними, добре дослідженими технологіями. А для генерації ключа шифрування використовуються дії користувача: хаотичні натискання клавіш на клавіатурі та хаотичні рухи мишою. Цей підхід сьогодні вважається оптимальним, оскільки він повністю виключає залежність надійності системи захисту від якості генератора випадкових чисел. Сам ключ шифрування за замовчуванням зберігається на жорсткому диску комп’ютера, і доступ до нього обмежений захистом паролем.

При першому налаштуванні BestCrypt Volume Encryption сканує систему та диск і далі відкривається початкова сторінка, яка зображена на рисунку 3.21:

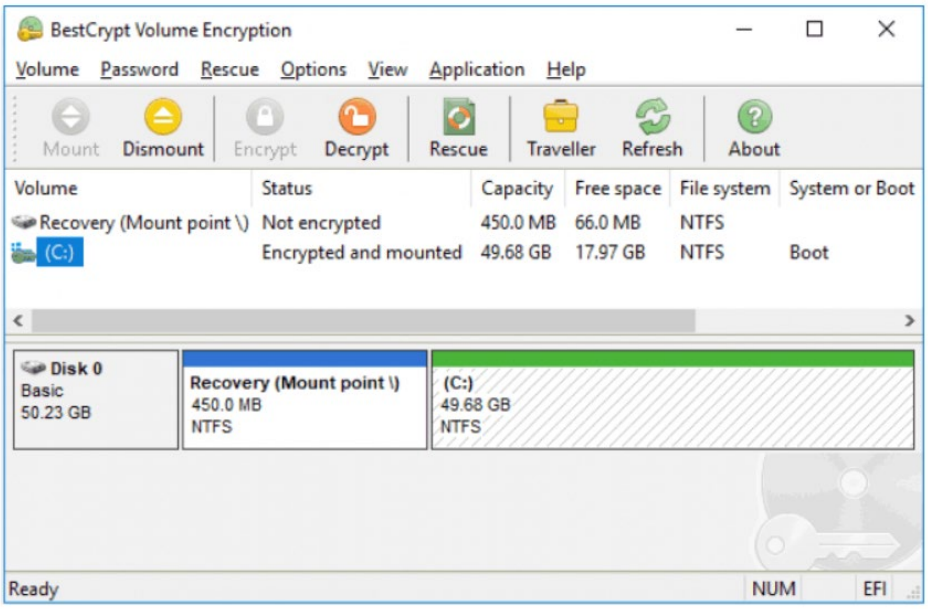

Рис. 3.21 Вікно програми BestCrypt Volume Encryption

Важливою особливістю BestCrypt Volume Encryption є можливість шифрування системного розділу жорсткого диска. Це дозволяє користувачам одночасно вирішувати кілька серйозних проблем. Для початку є можливість завантажити операційну систему, лише якщо відомий пароль для диску, який вже зашифрований. Програма дозволяє користувачеві вибрати тему, або іншими словами написи, які будуть видаватися при увімкненні ПК та неправильному введенні пароля. З шести тем два з них імітують різні помилки, які виникають при збоях операційної системи, і ще один - зупинений процес завантаження Windows. При їх використанні у людини, яка не знає про встановлений захист, створюється враження несправності комп'ютера, що є додатковим захистом.

Додатковою функцією програми BestCrypt Volume Encryption, яка буде дуже корисною для корпоративних користувачів, є підтримка роботи мережі. Якщо до шифрування на диску були спільні папки, то після їх відкриття всі дозволи відновлюються. Це дозволяє використовувати даний продукт для захисту будь-якої інформації на сервері: документів, баз даних.

5)Засіб захисту WEB-серверу

У файлі nginx.conf потрібно збільшити обмеження кількості файлів і відкритих з'єднань. Для початку необхідно налаштувати nginx для Web-серверу. У розділі http визначаємо потрібні параметри для роботи скрипта на мові Lua:

```
lua_shared_dict whitelist 100m;
lua_shared_dict banlist 1000m;
lua_package_path '/home/ Vladyslav/antiddos/?.lua;;';
init_by_lua ‘
local whitelist = ngx.shared.whitelist
whitelist:add("4.1.2.3", true)
whitelist:add("7.5.8.6", true) ;
access_by_lua_file /home/Vladyslav/antiddos/main1.lua;
```

Рис 3.22 Потрібні параметри для роботи скрипта

В рядку «lua_shared_dict» відповідає за створення значення ключа, іншими словами словнику. Це значення ключа однакове, тому в ньому зручно зберігати так звані «білі» та «чорні» списки. Цей словник також може використовувати параметр часу життя як додатковий параметр ключового значення, таким чином це ідеально буде підходити для зберігання лічильників шкідливого ПЗ, коли потрібно обмежити кількість запитів за певний проміжок часу.

В рядку «lua_package_path» визначаються шляхи для пошуку модулів Lua, в яких потрібно інтегрувати каталог зі скриптами. За допомогою двох крапок з комою в кінці рядка є можливість додати вказаний шлях до поточного значення шляху, а не змінювати його в цілому.

В рядку «init_by_lua» визначається код, який треба виконати один раз при запуску сервера, а не виконувати його в кожному новому запиті. За допомогою нього визначається білий список IP-адрес. Іншим параметром функції додавання є «true» це значення для використання його в операторі «if». Так як третього параметру часу життя немає тому використовується необмежений час.

Рядок «access_by_lua_file» визначає шлях до плану дій, які виконуються при кожному запиті до сервера.

Використовуючи середовище розробки ZeroBrane Studio, це середовище з відкритим кодом Lua для написання коду, виділенням синтаксису, аналізом коду, кодуванням у реальному часі та підтримкою налагодження для Lua 5.1, Lua 5.2, Lua 5.3, LuaJIT та інших механізмів Lua. ZeroBrane Studio використовує набір інструментів wxWidgets та компонент Scintilla для обробки файлів.

Реалізація скрипту для захисту Web-серверу від атак типу «відмова в обслуговуванні»

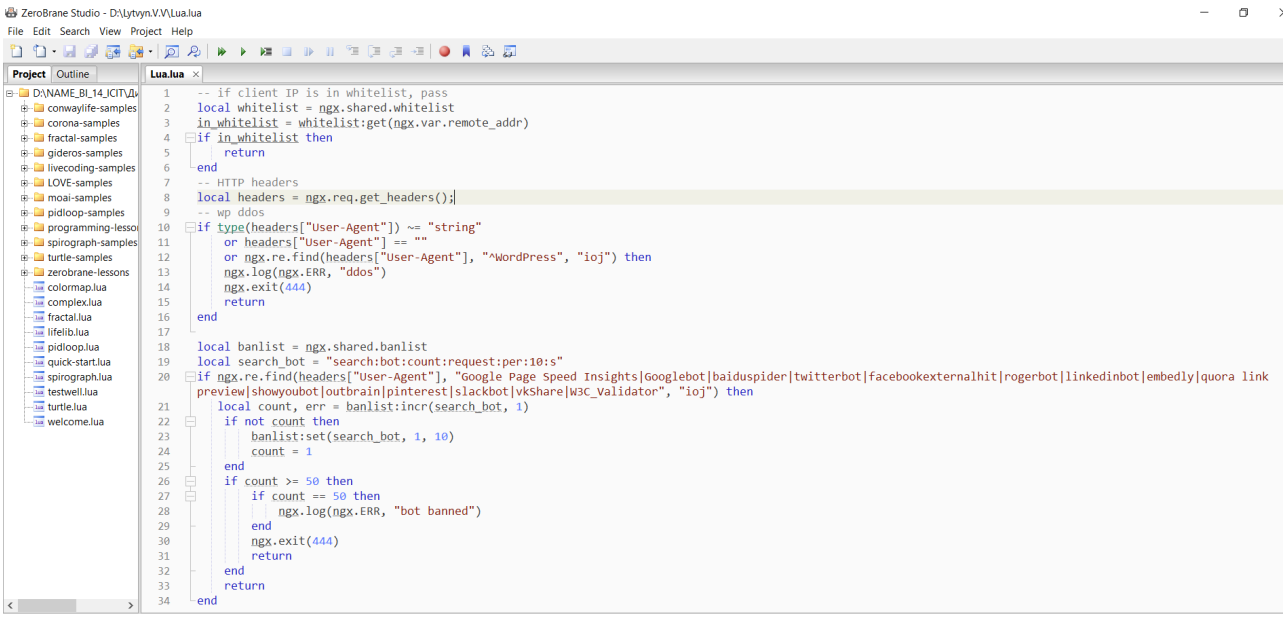

Рис.3.23 Скрипт захисту web-ресурсу

Глобальна змінна «ngx» застосовується для встановлення зв'язку з контекстом, який на сервері «nginx». Оператор «return» за тілом функції забезпечує повернення від модуля. Тобто, якщо IP-адреса присутня в списку дозволених, то скрипт припиняє роботу і продовжується робота запиту далі. Наступним кроком є виявлення атаки на основі специфікацій реалізації WordPress CMS. Якщо атака виявляється то робота закінчується помилкою 444: ngx.exit (444).

Далі відбувається пошук ботів. Тут потрібно застосувати лічильник, оскільки кіберзлочинці часто підробляють атаку під пошукового бота. «ban_list: set (search_bot, 1, 10)» розпочинає роботу лічильнику, який скине своє значення до нуля через десять секунд після початку роботи. «ban_list: incr (search_bot, 1)» додає значення 1. Тобто це лічильник, який буде рахувати кількість ботів.

Подальше виявлення ботів та зловмисників може відбуватися в різних напрямках. Скрипт базується на перевірках і також залежить від того факту чи підтримує клієнт переспрямування, налаштування файлів cookie та виконання коду.

Також таким чином можна використовувати так налаштований Web-сервер як проксі сервер, який буде захищати основний Web-сервер з іншою IP-адресою і фільтрувати запити IP-адрес та в результаті блокувати їх.

94.242.55.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	1	[]
82.146.36.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	1	[]
165.227.208.0			[]
46.173.218.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	18	[]
46.173.219.0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec...	15	[]
37.9.113.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
87.236.16.0	WordPress/5.2.4; http://seliane.ru	131	[]
157.55.39.0	msnbot/2.0b (+http://search.msn.com/msnbot.htm)	1	[]
5.45.207.0	Mozilla/5.0 (compatible; YandexMetrika/2.0; +http://yandex.com/bot...	2	[]
95.108.181.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
95.173.146.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/2010010...	1	[]
95.169.184.0	Zend\\Http\\Client	1	[]
188.127.249.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	6	[]
74.125.76.0	FeedBurner/1.0 (http://www.FeedBurner.com)	1	[]
52.162.161.0	Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot...	1	[]
87.250.224.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
141.8.142.0	Mozilla/5.0 (compatible; YandexMetrika/2.0; +http://yandex.com/bot...	2	[]
95.163.105.0	Mozilla/5.0 (Windows; Linux i686; en-us) like Gecko Safari/563.9	240	[]
95.108.213.0	Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)	1	[]
95.213.196.0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, l...	2	[]
94.242.57.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH...	11	[]
89.151.179.0	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, l...	1	[]
2.135.67.0	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHT...	1	[]
207.46.13.0	msnbot/2.0b (+http://search.msn.com/msnbot.htm)	2	[]
77.111.247.0	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHT...	1	[]
193.124.181.0	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko...	2	[]
199.249.230.0	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko...	2	[]

Рис. 3.24. Результат роботи скрипта.

6) Засіб фізичного захисту

До засобів фізичного захисту можна віднести біометричний захист робочих станцій Hamster Pro від Securegen.

Рис.3.25 Біометричний зчитувач Hamster Pro

Hamster Pro – це зчитувач з лінійки біометричних зчитувачів Secugen, яка набула особливої популярності на ринку завдяки тому, що має високу продуктивність, компактний розмір та відносно низьку ціну. Цей USB-сканер призначений для підвищення безпеки доступу до робочої станції або мережевих

ресурсів та веб-серверу. Зазвичай цей засіб застосовується для захисту робочих станцій з доступом до достатньо важливої інформації, такої як платіжні системи, дані пов’язані з інформацією про підприємство, особисті дані користувачів.

Оновлений пристрій реалізує підтримку Windows Biometric Framework (WBF), який дає можливість застосовувати Hamster Pro для автентифікації користувачів за допомогою відбитків пальців під час входу в операційну систему. Оптичний датчик, який вбудований в цей пристрій має розширення в 500 точок на дюйм. Особливістю пристрою є автоматична індикація сканування та розпізнавання недоліків, а також посилений захист від пошкоджень фізичних, тобто самого сканеру. Це робить цей пристрій оптимальним вибором для системи безпеки інформаційного ресурсу.

Процедура налаштування:

1.Зчитувач під’єднується до комп'ютера через порт USB-A і не потребує встановлення додаткового програмного забезпечення .

2.Всі драйвери, які необхідні для роботи пристрою завантажуються автоматично.

7)Засіб резервного копіювання та архівування.

Оптимальним рішенням для централізованого резервного копіювання даних на робочих станціях у корпоративній мережі є Acronis True Image - комплексний продукт для резервного копіювання інформації на робочих станціях, які є частиною комп’ютерної мережі підприємства. Ця програма дозволяє створювати резервні копії:

1) жорстких дисків та їх розділів включаючи всі дані, що зберігаються на них, а також операційні системи та додатки;

2) найважливіших для користувача файлів та папок.

Підтримка як 64-розрядної, так і 32-розрядної версій Windows забезпечує достатній захист даних на робочих станціях різних поколінь. У разі значної помилки програмного чи апаратного забезпечення робоча станція Acronis True Image дозволить провести повне відновлення системи або частково відновити окремі файли та папки, які необхідні користувачу. Система може бути

відновлена або до стану який був до помилки, або взагалі очищена і готова до використання знову.

Консоль управління Acronis, яка є частиною робочої станції Acronis True Image, також дозволяє віддалено адмініструвати всі комп'ютери в необхідній мережі: установку агентів (додатків, необхідних для резервного копіювання кожного комп'ютера), резервне копіювання та відновлення даних. Централізоване управління полегшує роботу системного адміністратора та значно зменшує загальні витрати на підтримку всієї корпоративної мережі.

Також існує ефективна технологія Acronis Drive Snapshot, яка за допомогою робочої станції Acronis True Image робить резервну копію даних не вимикаючи або перезапускаючи саму робочу станції, що дозволить не припиняти роботу персоналу. Якщо Acronis True Image створював резервні копії файлів по одному, то відкритий файл, швидше за все, буде змінено з моменту початку резервного копіювання, а потім збережено в резервній копії в інший момент часу і дані в резервній копії будуть суперечливими. Для усунення цього Acronis True Image створює так званий знімок, який фіксує дані для резервного копіювання до певного моменту часу.

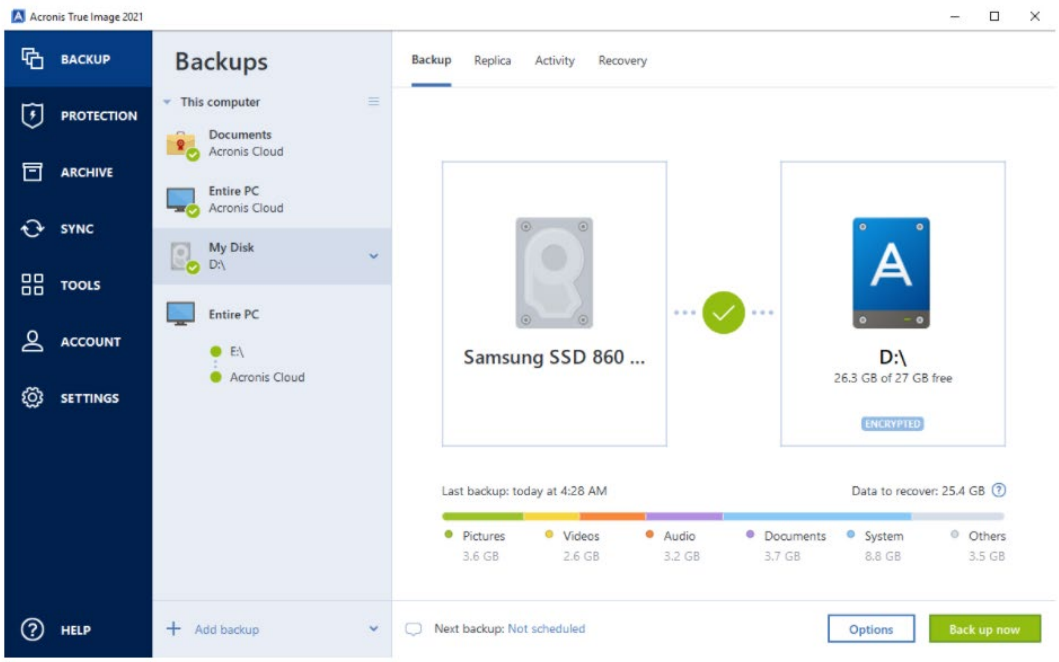

Рис. 3.26 Меню резервного копіювання в програмі Acronis True Image

Наступним кроком вибір параметри «New backup», тобто нового файлу бекапу.

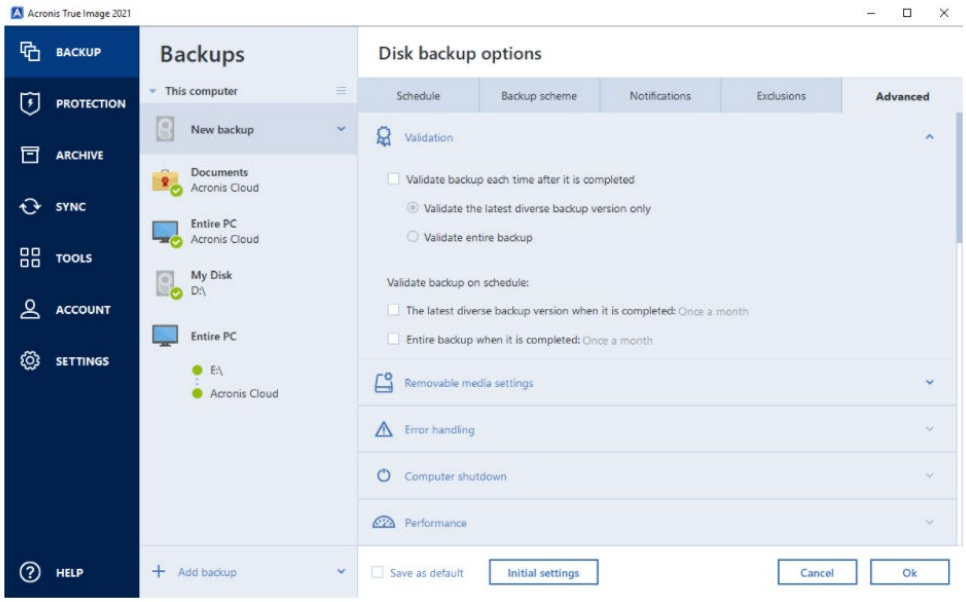

Рис. 3.27 Налаштування резервного копіювання Acronis True Image.

Процедура налаштування програми Acronis True Image:

Щоб створити резервну копію необхідно:

1.У головному меню обрати «Резервне копіювання» та натиснути «Змінити джерело». Далі необхідно вказати джерело резервної копії, наприклад, «Диски та розділи» далі «Локальний диск (C/D/E:)» , тобто необхідний для створення копії Також можна обрати «весь комп’ютер», «файли та папки», «мобільний телефон/планшет». Ще однією особливістю є те, що можна обрати «весь комп’ютер», «файли та папки», «мобільний пристрій» і будуть створені відповідні резервні копії.

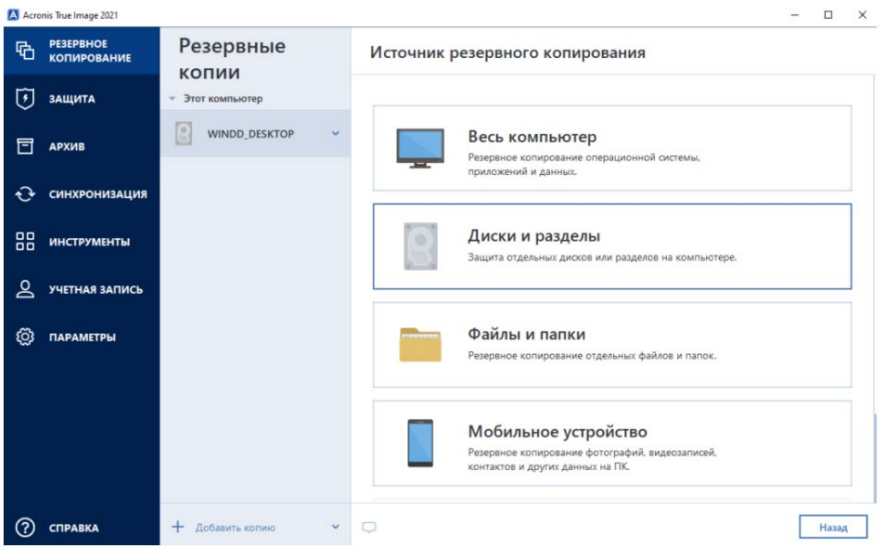

Рис. 3.28 Вибір джерела резервної копії

2. Далі необхідно вказати місце збереження резервної копії яка буде створена, натиснувши «Обрати пам’ять». Також є можливість зберегти на хмарне сховище Acronis Cloud або External Disk, тобто зовнішній жорсткий диск.

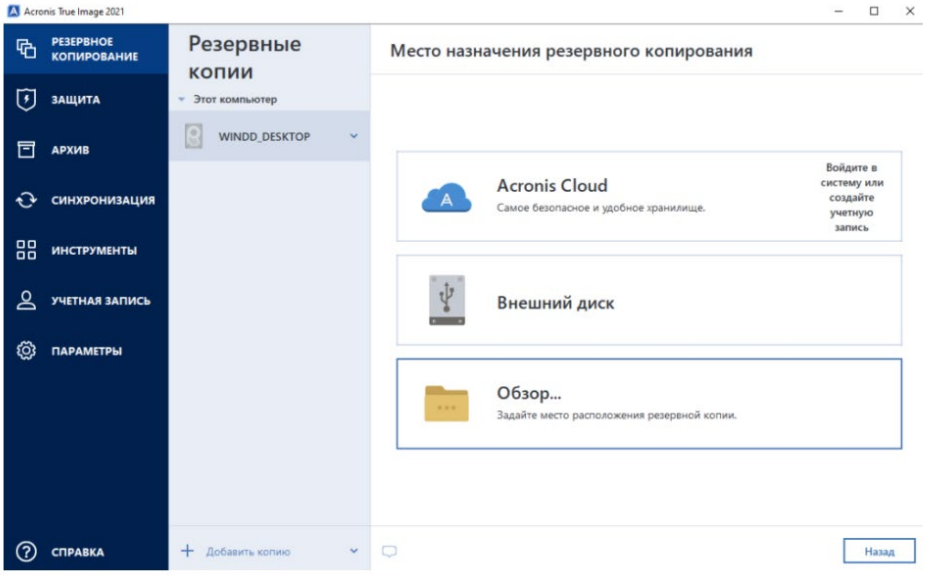

Рис. 3.29 Вибір місця збереження резервної копії.

3.У процесі вибору дисків для резервного копіювання необхідно увімкнути «Повний список розділів». Також позначити зарезервований системою диск, такий як «Диск бекапу», таким чином всі дані будуть зберігатися саме на цьому диску. Потім можна перейти до резервної копії, натиснувши «Створити копію».

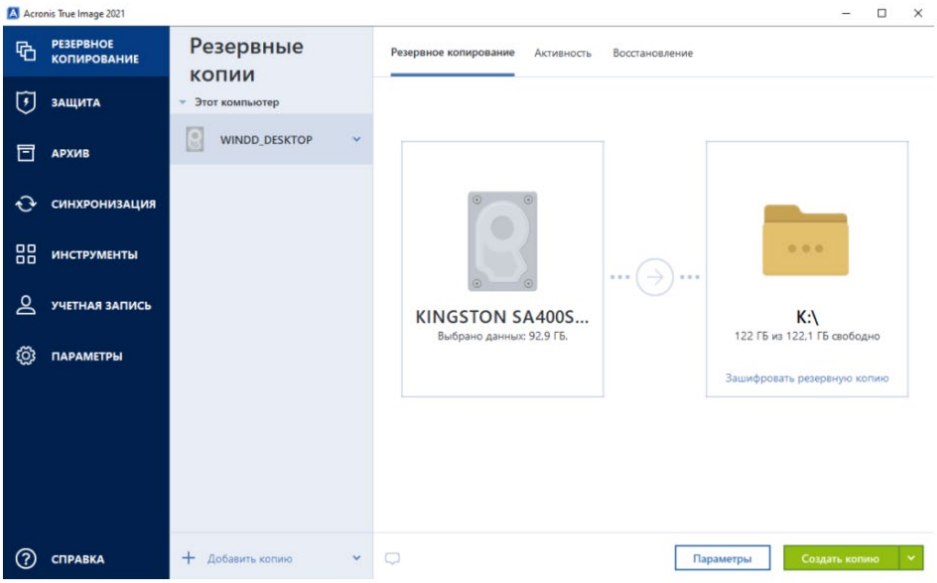

Рис. 3.30 Процес створення резервної копії.

Після цього створена резервна копія диску і в будь-який момент часу до неї можна повернутися за необхідністю.

3.3 Висновки до третього розділу

Створена система включає в себе 7 засобів , які захищають інформаційний ресурс від шкідливого програмного забезпечення, а також від різних видів загроз. Система зроблена з урахуванням загроз інформаційним ресурсам, а саме загрозам пов’язаними з шкідливим програмним забезпеченням. Також система використовує тільки ліцензійне програмне забезпечення, що дає можливість своєчасно оновлювати бази нового шкідливого ПЗ і адаптуватись до їх захисту. Також система використовує комплексні підходи до захисту інформаційних ресурсів та використовує набір методів та засобів які використовуються для безпеки інформаційного ресурсу. Засіб резервного копіювання та архівування яка захищатиме інформаційні ресурси від можливого шкідливого впливу програмного забезпечення, яке видаляє інформацію або змінює її, засіб фізичного захисту яка захищає від фізичного доступу зловмисника до інформаційного ресурсу, засіб криптографічного захисту інформації який про шкідливе ПЗ на ПК, засіб автентифікації і авторизації дозволяє шифрувати інформаційні ресурси для їх зберігання і захисту від шкідливого ПЗ, програмний модуль захисту WEB-серверу від шкідливого програмного забезпечення, засіб міжмережевого екранування який захищатиме інформаційний ресурс від шкідливого ПЗ яке може потрапити на робочу станцію через мережу інтернет, антивірусний засіб, який буде в режимі реального часу захищати і сповіщати користувачів користувачів захищатиме робочі станції від НСД з метою встановлення шкідливого ПЗ.

ВИСНОВКИ

У сучасному світі інформаційний ресурс став одним із найпотужніших важелів економічного розвитку підприємств та звичайних громадян. Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху для будь-якого бізнесу. Монопольне володіння певною інформацією або ресурсом дуже часто є великою перевагою в конкурентній боротьбі і, таким чином, зумовлює високу ціну інформаційного фактора. Широке впровадження персональних комп'ютерів вивело рівень інформатизації ділового життя на якісно новий рівень. Сьогодні важко уявити фірму чи підприємство, яке б не застосовувало сучасні засоби обробки та передачі інформації. Інформаційні ресурси накопичують значні обсяги інформації на носіях даних, що представляють велике значення для його власника .

Проаналізувавши існуючі системи захисту інформаційного ресурсу можна зробити висновок, що переважно розробляються часткові системи інформаційних ресурсів, які захищаються за допомогою одного метода або двох методів забезпечення захисту. Однак з бурхливим зростанням небезпечного програмного забезпечення для інформаційних ресурсів з'явилось питання підвищення системи захисту інформації та інформаційних ресурсів.

Було виявлено ряд недоліків існуючих систем які використовуються для захисту інформаційних ресурсів, а саме:

−недостатня кількість методів, які застосовуються для захисту;

−використання тільки одного засобу захисту від шкідливого ПЗ;

−відсутність комплексного підходу до захисту інформаційного ресурсу;

Результатом виконаної роботи являються розроблені та використані засоби та система захисту інформаційних ресурсів. Під час виконання роботи було:

1)Проведено аналіз інформаційних ресурсів і класифіковано їх, було досліджено існуючі підходи, засоби та методи захисту інформаційних ресурсів. Зроблено висновок, що необхідна комплексна система захисту інформаційних ресурсів від

шкідливого програмного забезпечення.

2)Створено систему захисту інформаційних ресурсів за допомогою фізичних, апаратних та програмних засобів забезпечення безпеки інформаційних ресурсів. Виходячи з першого завдання було застосовано актуальні засоби та методи захисту інформаційних ресурсів від шкідливого програмного забезпечення, а саме засіб апаратного міжмережевого екрану, програмний засіб захисту Web-ресурсу, засіб антивірусного захисту, комплекс криптографічного та фізичного захисту, засіб ідентифікації та авторизації, застосунок резервного архівування та копіювання.

3)Досліджено створену систему захисту інформаційного ресурсу. Описано та обґрунтувано вибір програмного та апаратного забезпечення, а також протестовано засоби захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1)Блюмин А.М. Мировые информационные ресурсы: Учебное пособие / А.М. Блюмин, Н.А. Феоктистов. — М.: Издательско-торговая корпорация "Дашков и Ко", 2011. – 296 с.

2)Васина Е.Н. Информационные ресурсы и документальные базы данных: создание, использование и анализ / Е.Н. Васина, О.Л. Голицына, Н.В. Максимов, И.И. Попов.— М.: РГГУ, 1997. – 209 с.

3)Введение в правовую информатику. Справочные правовые системы Консультант Плюс: Учебник для вузов / Под общ. ред. Д.Б. Новикова и В.Л. Камынина. — 33е изд., доп. и испр. — М.: ООО НПО “Вычислительная математика и информатика”, 2000. –319 с.

4)Леонтьев, Б.В. Мировые информационные ресурсы / Б.В. Леонтьев. — М.: Наука, 2001.-156 с.

5)Про Національну програму інформатизації [Текст]: Закон України № 74/98-ВР від 04.02.1998 / Верховна Рада України // Відомості Верховної Ради України.- 1998. –№ 27-28. –ст.181.

6)Державна політика в галузі управління інформаційним ресурсом України 2005 року [Електронний ресурс] : автореф. дис. ... д-ра політ. наук : спец. 23.00.02 / Соснін Олександр Васильович ; Одес. нац. юрид. акад. – Одеса, 2005. – 36 с. – Режим доступу: World Wide Web . – URL http://dspace.onua.edu.ua/bitstream/handle/11300/1612/Соснін%20 О.%20В.pdf?sequence=1&isAllowed=y.

7)Додонов О.Г. Інформаційні потоки в глобальних комп'ютерних мережах. / Додонов О.Г., Ланде Д.В., Путятін В.Г. — К. : Наукова думка, 2009. — 295 с.

8)Цирлов В.Л. Основы информационной безопасности автоматизированных систем. краткий курс / Цирлов В.Л . —М. : Изд-во Феникс 2008. — 253 с.

9)Казанцев С. Я. Правовое обеспечение информационной безопасности: учеб. Пособие для студ. высш. учеб. заведений/(С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский); под ред. С. Я. Казанцева. – 2-е изд., испр. и доп. – М.: Издательский центр «Академия», 2007. – 240 с.

10)Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей:

учеб. пособие/ Шаньгин В. Ф. – М. : ИД «Форум»: Инфра-М, 2008 – 416 с.

11)Сёмкин С.Н Основы организованного обеспечения информационной безопасности объектов информатизации./ Сёмкин С.Н, Э. В. Беляков, С. В. Гребенев, В. И. Козачок – М.: Изд-во «Гелиос АРВ» 2005. – 186 с.

12)Белов Е. Б. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

13)Rick Lehtinen, Deborah Russell, G. T. Gantemi Sr. Computer Security Basics O'Reilly, 2006. – 312 p

14)Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учеб.-справ/М.А. Иванов.-М.: КУДИЦ- ОБРАЗ, 2001. -365 с

15)Джонс К.Д. Инструментальные средства обеспечения безопасности/К.Д. Джонс, М. Шема, Б.С. Джонсон.- М.: ИНТУИТ, 2007.-1028 с.

16)P. Mahalanobis, "On the generalized distance in statistics," Proceedings of the National Institute of Science, 1936. – 49–55 p

17)Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие/В.А. Глатенко.- ИНТУИТ, 2006.-264 с.

18)Малюк А.А. Введение в защиту информации в автоматизированных системах/ А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия Телеком, 2001. – 178 с

19)Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин., Е.В.Куренков, А.В. Лысов. - СПб.: Полигон, 2000. – 886 с

20)Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов/ П.Ю. Белкин, О.О. Михальский, А.С. Першаков. – М.: Радио связь, 2000.- 215 с.

21)Аверченков В.И. Криптографические методы защиты информации/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак, – Брянск: БГТУ, 2010. – 216 с.

22)Аверченков В.И. Организационная защита информации: учеб. Пособие для

вузов / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 184 с.

23)Болдырев А.И. Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практ. Пособие/ А. И. Болдырев – М.: НЕЛК, 2001. – 137 с.

24)Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

25)Бабак В.П. Інформаційна безпека та сучасні мережеві технології : Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – Київ : Издательство НАУ, 2003. – 670 с.

26)Хадиаров Г. Г. Структура информационных ресурсов для бизнеса // Актуальные проблемы Европы. Информационное обеспечение бизнеса: Опыт Западной Европы и США: Сб. науч. тр. РАН ИНИОН. Центр науч..информ. исслед. глобал. и регион. Проблем. Отд. Зап. Европы и США/ Ред..сост. А. К. Субботин. — М.: ИНИОН РАН, 2004. —С. 94–104.

27)Хорошилов А. В. Управление информационными ресурсами / А. В. Хорошилов, С. Н Селетков, Н. В. Днепровская— М.: Финансы и статистика, 2006.

28)Мак-Клар С. Секреты хакеров. Безопасность сетей / С. Мак-Клар, Дж. Курц, Дж. Скембрей. - 4-е изд.. - М.: Вильямс, 2004. - 656 с.

29)Обзор технологий идентификации и аутентификации [Электронный ресурс] / Алексей Сабанов – АДЭ №7, 2006. – Режим доступа: World Wide Web. – URL: https://www.aladdinrd.ru/company/pressroom/articles/obzor_tehnoogij_identifikacii_i_autentifikacii

30)McCollum K. Cornel University Offers Developing Nations Digital Journals on Agriculture / McCollum K –Ithasa, 1999– 50 p.

31)Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища: [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2014. – 296 с.

32)Про науково-технічну інформацію [Текст]: Закон України від 25.06.1993 р. №

3322-XII [Електронний ресурс] // Інформаційне законодавство. Основні нормативні акти / уклад.: Р. С. Кірін, С. В. Грищак, Д. О. Шашенко. – Дніпропетровськ : Нац. гірн. ун-т, 2012. Ч. 3. – 264 с. – С. 13–19. – Режим доступа: World Wide Web: http://ir.nmu.org.ua/bitstream/handle/123456789/2128/%D0 %9 D%D0 %A2 %D0 %91452169.pdf?sequence=1.