Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації
(повна назва)

Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Комплексна система захисту електронних інформаційних ресурсів підприємства
(тема)

Виконав:
студент 2 курсу, групи СТЗІАм-21-1
Тарасенко Б. В.
(прізвище, ініціали)

Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Системи технічного захисту інформації, автоматизація її обробки
(повна назва освітньої програми)

Керівник проф. Милютченко І. О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Антіпов І.Є.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет_Інформаційних радіотехнологій та технічного захисту інформації_
Кафедра_Комп'ютерної радіоінженерії та систем технічного захисту інформації_
Рівень вищої освіти __другий (магістерський)_____
Спеціальність _____125_____Кібербезпека _____

Тип програми _____освітньо-професійна _____
Освітня програма _____Системи технічного захисту інформації,_____
_____автоматизація її обробки_____

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові_____Тарасенку Богдану Вячеславовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи Комплексна система захисту електронних інформаційних ресурсів на підприємстві
затверджена наказом університету від _04_ _____11_____2022 р. _ № 1446Ст
2. Термін подання студентом роботи до екзаменаційної комісії _10_ _12__ 2022 р.
3. Вихідні дані до роботи Система має забезпечувати комплексний захист електронних інформаційних ресурсів (ЕІР) на підприємстві та складатися з підсистем: захисту інформації від витоку технічними каналами, охоронної сигналізації, контролю та управління доступом, збору та обробки інформації тощо. Система має забезпечувати захист від DDoS-атак. Функціонування КСЗІ має забезпечувати служба захисту інформації. Штатна чисельність підприємства _30 осіб, сфера діяльності – надання юридичних послуг
_____
4. Перелік питань, що потрібно опрацювати в роботі _____
1 Поняття, визначення та класифікація ІР та ЕІР. 2 Структура ІР та ЕІР підприємства. 3 Методи та засоби захисту ЕІР від DDoS-атак. 4 Підприємство як об'єкт інформаційної діяльності. 5 Вибір структури КСЗІ підприємства. Висновки._____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

1. Класифікація IP.
2. Класифікація EIP.
3. Структура IP підприємства.
4.Завдання КСЗІ підприємства.
5-6. Методи та засоби захисту від DDoS-атак.
7. План ОІД.
8. Підсистеми КСЗІ.
9. Засоби захисту ПЗ підприємства.
10. Схема розміщення технічних засобів захисту приміщення.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів	Примітка
1	Огляд літератури	02.11 - 05.11	
2	Аналіз поняття і класифікації EIP	06.11 - 08.11	
3	Формування структури EIP на підприємстві	09.11 - 12.11	
4	Розробка структурної схеми КСЗІ підприємства	13.11 - 20.11	
5	Складання функціональних схем підсистем КСЗІ	21.11 - 29.12	
6	Складання плану розміщення засобів технічного	30.11 - 03.12	
	захисту		
7	Оформлення графічних матеріалів та пояснювальної	04.12 - 10.12	
	записки		
8	Подання на рецензування та антиплагіатну перевірку	11.12 - 15.12	

Дата видачі завдання _29_ ____09_____2022 р.

Студент _____
(підпис)

Керівник роботи _____ _____ проф. Милютченко І.О.___
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 84 с., 15 рис., 6 табл., 1 додаток, 31 джерело.

ЗАХИСТ, ІНФОРМАЦІЙНІ РЕСУРСИ, ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, ЕЛЕКТРОННІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.

Об’єкт дослідження – інформаційні ресурси підприємства.

Предмет дослідження – комплексна система захисту інформаційних ресурсів підприємства .

У роботі розглянуто визначення інформаційних ресурсів, структура інформаційних ресурсів, засоби захисту електронних ресурсів від DDoS-атак, несанкціонованого доступу та засоби технічного захисту інформації. Розглянуто підприємство, яке надає юридичні послуги громадянам, зроблено аналіз можливих каналів витоків інформації.

У роботі запропоновано комплексний захист електронних інформаційних ресурсів підприємства у сфері надання юридичних послуг.

Галузь використання – системи технічного захисту інформації.

ABSTRACT

Explanatory note of the qualification work: 84 p., 15 fig., 6 tab., 1 application, 31 sources.

PROTECTION, INFORMATION RESOURCES, ELECTRONIC INFORMATION RESOURCES, TECHNICAL MEANS OF INFORMATION PROTECTION, ELECTRONIC MEANS OF INFORMATION PROTECTION.

The object of research is information resources of the enterprise.

The subject of the study is a comprehensive system of protection of information resources of the enterprise.

The work considers the definition of information resources, the structure of information resources, means of protecting electronic resources from DDoS attacks, unauthorized access, and means of technical information protection. An enterprise that provides legal services to citizens was considered, and an analysis of possible channels of information leaks was made.

The work proposes comprehensive protection of electronic information resources of the enterprise in the field of providing legal services.

Field of use – technical information protection systems.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА АБРЕВІАТУР

АТС – автоматична телефонна станція
ВЧ – високочастотні
ДТЗС – допоміжні технічні засоби і системи
ЗТР засоби технічної розвідки
ІзОД – інформація з обмеженим доступом
ІС – інформаційна система
КЗ – контрольована зона
КСЗІ – комплексна система захисту інформації
ОІД – об’єкт інформаційної діяльності
ОТЗ – основні технічні засоби
ПБ – політика безпеки
ПЕМВН - побічні електромагнітні випромінювання і наводки
ПЕОМ – персональна обчислювальна машина
ПЗ – програмне забезпечення
ПК - персональний комп’ютер
ТЗ – технічні засоби
ТЗПІ - технічні засоби прийому, обробки, зберігання та передачі інформації
ТП – трансформаторна підстанція
ТР – технічна розвідка
ACK – acknowledge
ACL – access control list
AES – advanced encryption standard
ARP – address resolution protocol
ASCII – american standard code for information interchange
AWS – amazon web services
CDN – content delivery network
DDoS – distributed denial of service
DNS – domain name system
DoS – denial of service
HTTP – hypertext transfer protocol
HTTPS – hypertext transfer protocol secure
ICMP – internet control message protocol

IP – internet protocol
MAC – media access control
OSI – the open systems interconnection model
PAP – password authentication protocol
RIP – routing information protocol
RPC – remote procedure call
SSL – secure sockets layer
SYN – synchronize sequence numbers
TCP – transmission control protocol
UDP – user datagram protocol
UPnP – universal plug and play
URL – uniform resource locator
VPN – virtual private network
VPS – virtual private server
WAF – web application firewall
WPA2 – wi-fi protected access

ВСТУП

У сучасному суспільстві інформація стає найбільш важливою цінністю, а індустрія отримання, обробки і трансляції інформації – провідною галуззю діяльності, куди з кожним роком вкладають все більш значні капітали.

Інформаційні ресурси виступають важливим, необхідним елементом економічних, політичних, правових та інших суспільних процесів. Інформація в різних формах і вигляді включена до ринкових відносин.

Виникли тенденції неухильного перекачування трудових ресурсів зі сфери матеріального виробництва в інформаційну сферу. Національні інформаційні ресурси — це нова економічна категорія. Інформація стає таким самим ресурсом, як матеріал та енергія.

Для нормального функціонування організації будь-якого масштабу недостатньо мати матеріальні, фінансові та людські ресурси — необхідно знати, що з цим усім треба робити, знати про технології їх використання. Тому інформація, інформаційні ресурси нині розглядаються як окрема економічна категорія.

Управління інформацією є, по суті, управлінням соціальними й економічними процесами. Через це проблеми розповсюдження інформації, широкого її використання набувають не лише суто економічного, а й політичного характеру як у межах окремої країни, так і на міжнародній арені. Інформаційні ресурси суспільства характеризують загальний рівень розвитку продуктивних сил і передусім самої людини. Тому не випадково, що найбільш жорстка конкуренція у світі в сучасних умовах відбувається саме у сфері науки, виробництва знань, бо лідерство у цій сфері в кінцевому результаті забезпечує лідерство і в усіх інших сферах діяльності, включаючи економічну та військову.

Витік інформації є серйозною небезпекою для багатьох підприємств. Він може статися в результаті наміру третіх осіб або з необережності співробітників. Навмисна організація витоку відбувається з двома цілями: першою з них стає нанесення шкоди державі, суспільству або конкретному підприємству, ця мета характерна для проявів кібертероризму; другою метою є отримання переваги в конкурентній боротьбі.

Ненавмисний витік відбувається найчастіше через необережність співробітників організації, але також може привести до серйозних несприятливих наслідків. Створення системи захисту інформаційних активів від втрати в

компаніях всіх типів повинні здійснюватися на професійному рівні, з використанням сучасних технічних засобів. Для цього необхідно мати уявлення про канали витоку і способах блокування цих каналів, а також про вимоги, що пред'являються до сучасних систем безпеки.

Витік інформації є серйозною небезпекою для багатьох підприємств. Він може статися в результаті наміру третіх осіб або з необережності співробітників. Навмисна організація витоку відбувається з двома цілями: першою з них стає нанесення шкоди державі, суспільству або конкретному підприємству, ця мета характерна для проявів кібертероризму; другою метою є отримання переваги в конкурентній боротьбі.

У наші дні всі компанії, що мають зв'язок із забезпеченням інформаційної безпеки та протидії кібератакам, помітили великий зріст кількості DDoS-атак і їх потужність.

Дуже часто можна почути про неефективність засобів захисту та протидії цим атакам, бо періодично ми чуємо повідомлення в засобах масової інформації про недоступність тих чи інших ресурсів у результаті розподілених атак, спрямованих саме на відмову в обслуговуванні. Також у наш час атаки вже ведуться не тільки на величезні компанії, але і на невеликі сайти, які раніше не піддавалися таким атакам і увазі зловмисників. Тому у даний час ці невеликі, через їх затребуваність, проблеми з їх роботою можуть бути дуже критичними для нас. Тобто мотиви, які рухають зловмисниками, повністю змінились. Якщо раніше DDoS-атаки визивались заради протестів або хуліганства, то сьогодні вони вже все частіше використовуються для шантажу або як спосіб вимагання грошей. Тобто DDoS-атаки переросли з одиночних протестних акцій вже у великий кримінальний бізнес, який не обмежується тільки вимаганням грошей, але й інструментом терористичних операцій. Зараз у всьому світі дуже часто відбуваються атаки на сайти державної влади напередодні будь-яких великих подій, які пов'язані з інтернет ресурсами.

Якщо визвати відмову у роботі великого ресурсу, який має у своєму арсеналі активні засоби протидії, можна зробити тільки з допомогою заповнення всієї полоси пропускання каналу зв'язку, що надає причину для створення та підтримки великої бот-мережі. У цей же час для паралізації невеликого регіонального ресурсу для котрого буде достатньо досить невеликої по потужності атаки і як наслідок з цього, використання невеликої бот мережі. Так як обслуговування та підтримка

таких бот-мереж є менш витратним, і потенційно такі бот-мережі може зробити більша кількість зловмисників. Цей факт на тлі відсутності адекватних засобів протидії робить загрози безпеки регіональних ресурсів в результаті DDoS-атак особливо значущим. З одного боку, для протидії таким атакам можуть бути ефективно застосовані засоби, призначені для відбивання великих атак. З іншого - впровадження і підтримка таких коштів економічно затратно і не по кишені регіональних ресурсів. Засоби протидії, спеціалізовані саме на забезпечення безпеки невеликих і середніх ресурсів, отримали менший розвиток через переважання в минулому саме великих атак. І в даний час відстають від еволюції самих DDoS-атак.

1 ПОНЯТТЯ, ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ ІР ТА ЕІР

Інформаційні ресурси - у широкому сенсі - сукупність даних, організованих для ефективного отримання достовірної інформації [7].

Це книги, статті, патенти, дисертації, науково-дослідна та дослідно-конструкторська документація, технічні переклади, дані про передовий виробничий досвід і ін

Інформаційні ресурси (на відміну від усіх інших видів ресурсів - трудових, енергетичних, мінеральних і т.д.) тим швидше ростуть, чим більше їх витрачають.

Ресурси - це наявні в наявності запаси, кошти, які можуть бути використані при необхідності. В даний час учені і практики відносять інформаційні ресурси до важливих стратегічних ресурсів, від яких залежить розвиток економіки, науки, освіти, культури і т.д. Перші спроби дати визначення інформаційних ресурсів були зроблені в 90-і роки XX століття, коли оформився так званий "ресурсний підхід" до вивчення інформації. У наш час термін "інформаційні ресурси" є загальновживаної. Але, незважаючи на це, точного визначення його немає. Використовується вузьке та широке розуміння інформаційних ресурсів: у вузькому розумінні маються на увазі тільки мережеві інформаційні ресурси, доступні через комп'ютерні засоби зв'язку, а в широкому - будь-яку зафіксовану на традиційних або електронних носіях інформацію, придатну для збереження і поширення [7].

У більш конкретному вигляді під інформаційними ресурсами розуміють організовану сукупність інформації, інформаційних продуктів та інформаційних технологій, які призначені для інформаційного забезпечення життєдіяльності людини, суспільства та держави. Тому, книги (найперші інформаційні ресурси), музеї, бібліотеки, архіви тощо – все це інформаційні ресурси.

Структуру інформаційних ресурсів складають масиви документів, окремі документи тощо, в яких накопичується та зберігається сформована за певними ознаками або критеріями інформація.

В науковій літературі пропонується багато засад для класифікації інформаційних ресурсів.

Так, за природою інформації, яка їх створює, інформаційні ресурси поділяються на такі, що створюються зі штучної інформації та інформації, яка утворюється самостійно, незалежно від людини.

Перший клас інформаційних ресурсів створює інформація, яка утворюється самостійно. Наприклад, інформація про чисельність населення в країні, інформація гідрометцентру тощо.

До другого класу інформаційних ресурсів відноситься інформація, яка створюється штучно в результаті інтелектуальної діяльності людини. Наприклад, математична, логічна обробка інформації, літературні твори тощо. При цьому процес творчості припускає не тільки переробку вже відомої інформації, а й створення нової інформації – прогнозів, винаходів тощо.

За сферами використання інформаційні ресурси поділяються на бібліотеки, архіви, фонди інформації, електронні інформаційні системи тощо. В основі цієї класифікації лежать інтереси споживачів інформації. Споживач відноситься до інформації як до джерела своїх знань, яким він користується у повсякденному житті, під час отримання освіти, професійної підготовки, перепідготовки тощо. При цьому відбувається формування інформаційних ресурсів з урахуванням потреб споживачів.

За способам формування інформаційних масивів і розповсюдження інформації з них інформаційні ресурси поділяються на стаціонарні і мобільні.

Стаціонарні інформаційні ресурси формуються і використовуються, як правило, в спеціалізованих інформаційних організаціях за допомогою їх інформаційних систем і мереж, у том числі й через Інтернет. Основний механізм розповсюдження інформації з таких інформаційних ресурсів реалізується в порядку надання інформаційних послуг, тобто через пошук інформації в інформаційних системах цих організацій при зверненні до них користувачів (споживачів). Причому це може здійснюватися як безпосередньо самим користувачем, якщо такі можливості надаються йому відповідною інформаційною системою, так і через посередника. Споживач повинен знати місце розташування інформаційної організації і умови отримання інформації з її ресурсів. Такий механізм отримання інформації з інформаційного ресурсу заснований на принципі: споживач рухається до ресурсу.

Пересувні (або їх ще називають мобільними) інформаційні ресурси формуються державними і приватними (комерційними) інформаційними організаціями як спеціальні інформаційні продукти, головним чином, у вигляді банків даних. Такі інформаційні продукти тиражуються і розповсюджуються в комплексі - банк даних включає в свій склад і базу даних, і пошуковий апарат до

неї. Інформаційні ресурси ще можна класифікувати за видами інформації, з якої вони складаються. З огляду на це існують інформаційні ресурси [7]:

- правової інформації;
- науково-технічної інформації;
- політичної інформації;
- фінансово-економічної інформації;
- статистичної інформації;
- інформації про стандарти і регламенти, метрологічної інформації;
- соціальної інформації.

У більш розширеному варіанті поділ на групи може здійснюватися з урахуванням додаткових критеріїв. І в першу чергу тут потрібно відзначити, що на сучасному етапі розвитку суспільства поняття інформації, або ІР, нерозривно пов'язане з документуванням (це так звана документована інформація). Мається на увазі, що дані будь-якого типу фіксуються або зберігаються на певному типі носія (друковані, комп'ютерні носії, сервери, канали зв'язку тощо). На рис. 1.1 наведено приклад класифікацій інформаційних ресурсів.

Рисунок 1.1 – Класифікація інформаційних ресурсів

Якщо говорити про основні напрямки в поділі ІР на класи за якимись критеріями, можна зустріти досить багато різних уявлень. Однак серед всіх тих ознак, за якими проводиться класифікація інформаційних ресурсів, можна виділити найосновніші: за джерелом створення; за ступенем доступу; за цільовим призначенням; за способом подання та виду носія; за формою власності; за методом організації та зберігання; за змістом; за мовною і національно-територіальною або географічною ознакою; за рівнем компетенції і т. д. Самим великим класом серед всіх є ознака змісту. Про це буде сказано окремо. Розглянемо інші розділи. Серед джерел створення ІР розрізняють первинні і вторинні. Сюди ж відноситься поділ на правову і неправову (недокументовану) інформацію, яка залишається поза полем регулювання з точки зору юридичних норм.

У поділі на основі доступу це може бути публічна або приватна інформація з обмеженим доступом (наприклад, державна, службова, комерційна таємниця або особисті дані). В цільовому призначенні найчастіше виділяють наступні інформаційні ресурси: особисті; корпоративні; бізнес-ресурси; ЗМІ; політичні; освітні; культурні; ресурси організацій і установ; послуги і сервіси; розваги; спорт; відпочинок; дошки оголошень; зберігання і мультимедіа і т. д. Тепер подивимося, які параметри використовуються для класифікації інформаційних ресурсів за способом подання.

Інформаційні ресурси за способом доступу поділяються на інформаційні ресурси, які складаються з інформації відкритого доступу (без обмеження); інформації з обмеженим доступом (державна таємниця, конфіденційна інформація, комерційна таємниця, банківська та інші види таємниць, персональні дані).

За видом носія інформації інформаційні ресурси формуються на традиційному носії – папері, на комп’ютерних носіях інформації, в пам’яті комп’ютера, на сервері тощо.

За способом організації зберігання і використання інформаційні ресурси поділяються на традиційні (масив, фонд документів, архів) та автоматизовані (Інтернет, банк даних, автоматизована інформаційна система (мережа), база знань.

За формою власності інформаційні ресурси можуть мати статус загальноукраїнського національного надбання, державної власності, приватної власності, колективної власності.

Ще одну класифікацію інформаційних ресурсів можна провести по видах джерел інформації та сферами їх використання. За цими підставами інформаційні

ресурси поділяються на ресурси науково-технічної інформації, соціально-економічної, правової, освітянської, соціально-культурної тощо.

1.1 Електронні інформаційні ресурси

Електронний інформаційний ресурс – це інформаційний ресурс, який зберігається в електронному чи комп'ютеризованому форматі та може бути досягнутий, знайдений та перетворений засобами електронної мережі або іншої електронної технології обробки даних. Будь-який електронний інформаційний ресурс включає такі аспекти поняття, як цифрова форма фіксації інформаційних даних, комп'ютерні засоби та програмне забезпечення для відтворення та керування, електронне середовище для розповсюдження (комп'ютерні мережі та засоби сучасного телекомунікаційного зв'язку) [23].

Електронні інформаційні науково-освітні ресурси — це електронні ресурси, які наповнюють науково-освітній інформаційний простір з метою цільового їх використання.

Розробка і впровадження автоматизованих інформаційних систем, а також новітніх інформаційних технологій зумовили появу наступних електронних інформаційних ресурсів: баз даних, електронних видань, мультимедіа та гіпертекстових систем.

До переваг електронних інформаційних ресурсів, можна віднести:

1) можливість проводити пошук не тільки за однією ознакою, як це прийнято в масивах друкованих матеріалів, але одночасно з їх поєднанню в різних комбінаціях ознак;

2) можливість проводити пошук в режимі теледоступу одночасно до багатьох баз даних, використовуючи один і той же запит;

3) можливість негайного доступу до інформаційного ресурсу, в той час як друковані документи доходять до споживача протягом тривалого часу, що обчислюється місяцями після свого видання;

4) оперативність пошуку (особливо у великих масивах інформаційних ресурсів), яка скорочується до хвилин в порівнянні з традиційними методами, де витрачаються дні чи тижні;

5) результати пошуку забезпечують більшу точність вибірки, її глибину і повноту;

6) можливість отримати інформацію про зміст статті або книги ще до її публікації, тому що швидко впроваджується практика надання авторами авторефератів на опубліковані матеріали, які після прийняття їх журналами відразу надходять в бази даних.

Таким чином, один з головних аргументів на користь створення електронних інформаційних ресурсів – оперативний і широкий доступ до різноманітної інформації в різних областях діяльності людини, що веде до підвищення якості та ефективності результатів інформаційних технологій.

На рис. 1.2 наведені основні види електронних інформаційних ресурсів за різновидністю інформації, призначеної для сприйняття [23].

Рисунок 1.2 – Види електронних інформаційних ресурсів

Основний недолік електронного інформаційного ресурсу полягає в необхідності мати комп'ютер, але в сучасному світі, це не є великою проблемою, адже більша частина населення світу має комп'ютер та володіє навичками роботи з ним.

Електронні ресурси – це інформаційні ресурси, якими керує комп'ютер, у тому числі ті, що потребують використання периферійного пристрою, підключеного до комп'ютера.

Будь-який електронний інформаційний ресурс характеризується наявністю в ньому об'єкта, який є їх джерелом, суб'єкта, що їх використовує з метою вирішення різних управлінських чи економічних завдань.

Інформація про об'єкт набуває статуту електронного інформаційного ресурсу у випадку набуття змісту і форми, які можна використовувати в процесі управління та виробництва.

Також необхідно відмітити, що автоматизований пошук інформації надає користувачеві великі зручності в організації праці, а саме такі як автоматичне повторення запиту при поповненні баз даних, здатність швидкого замовлення першоджерела в онлайн-режимі та отримання результатів пошуку у вигляді машино читаного файлу, придатного до подальшої обробки (введення в персональну базу даних, підготовка звітів, статей, оглядів тощо).

Таким чином, один з головних аргументів на користь створюваних електронних інформаційних ресурсів – оперативний і широкий доступ до різноманітної інформації в різних областях діяльності людини, що веде до підвищення якості та ефективності результатів інформаційних технологій.

Електронні інформаційні ресурси класифікують за наступними, характерними для них критеріями, приклад яких наведено в таблиці 1.1.

Таблиця 1.1 – Класифікація електронних інформаційних ресурсів

№	Ознаки	Приклад електронних інформаційних ресурсів
1	За ступенем структурування	Від безперервного тексту, який не має розподілу на абзаци, параграфи тощо, до формального представлення інформаційних даних у базах даних
2	За типом ресурсу	– електронні дані; – електронні програми; – комбіновані: інтерактивні мультимедійні онлайнові служби.

Продовження таблиці 1.1

3	За типами носіїв електронних ресурсів	– локального доступу; – ресурси віддаленого доступу;
4	За технологією розповсюдження	– локальні електронні видання; – мережеві; – комбінованого розповсюдження.
5	За характером взаємодії з користувачем	– детерміновані електронні інформаційні ресурси; – недетерміновані ресурси.
6	За специфікою електронних ресурсів	– за цільовим призначенням; – за періодичністю; – за структурою; – за правовим статусом; – за наявністю друкованого еквіваленту.

2 СТРУКТУРА IP ТА EIP ПІДПРИЄМСТВА

Підприємства отримують інформацію багатьох різних типів у різних системах. Часто такі системи ростуть швидше у вигляді „як є”, ніж структурно, щоб швидко реагувати на нові потреби бізнесу. Результат часто виглядає у вигляді набору інформаційних ланцюгів, ізольованих один від одного і зовні не мають один до одного ніякого відношення. Між тим, багато елементів з цих даних пов’язані один з одним, і підприємство, яке зможе об’єднати і використовувати ці розрізнені джерела даних, отримає величезну перевагу.

Під інформаційним ресурсом підприємства розуміють сукупність нематеріальних активів, документів, що мають важливе стратегічне значення для функціонування організації. Інформаційні ресурси підприємства служать інструментами примусу або стимулювання виробничо-комерційної діяльності, прийняття управлінських рішень і навчання. Ресурс – запас, джерело чого-небудь.

Розглянемо джерела формування інформаційних ресурсів підприємства. Будь-яка організація існує в деякій зовнішньому середовищі. Ця ж організація породжує своє внутрішнє середовище. Внутрішнє середовище формується із сукупності структурних підрозділів підприємства і працюючих там людей технологічними, соціальними, економічними та іншими відносинами між ними. В залежності від джерела виникнення в рамках організації є внутрішня і зовнішня інформація, які складають її інформаційні ресурси. Інформація внутрішнього середовища, як правило, точна, повністю відображає фінансово- господарський стан підприємства. Її обробка часто-густо може здійснюватися за допомогою стандартних формалізованих процедур. Внутрішня інформація: про людей, продукти, витрати, скарги, послуги, технологічні процеси, сфери застосування продукту, методи збуту і техніки продажів, постачання, канали збуту.

Згідно із завданням, розглянемо підприємство, яке надає громадянам адміністративні послуги. На цьому підприємстві використовуються нормативні документи, бази даних клієнтів, вихідні документи, що надаються відвідувачам та технічна документація.

2.1 Нормативні документи

Нормативний документ – документ, що встановлює правила, загальні принципи чи характеристики щодо різних видів діяльності або їх результатів [18].

Нормативний документ є продуктом стандартизації.

Стандартизація – це діяльність з метою досягнення відповідного ступеня впорядкування у визначеній галузі шляхом установлення положень для загального та багаторазового використання, для вирішення існуючих або можливих задач.

Діяльність у галузі стандартизації відома ще з давніх часів. Розвиток економічних зв'язків між країнами та розширення робіт із стандартизації в промислово розвинених країнах вимагали відповідного регулювання.

Категорії нормативних документів зі стандартизації наведено на рис. 2.1.

Рисунок 2.1 – Категорії нормативних документів

Нормативні документи системи технічного захисту інформації визначає загальні вимоги до організації проведення на об'єкті інформаційної діяльності органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації випробувань щодо створення комплексу ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом технічними каналами [18].

НД встановлює засади щодо проведення випробувань з метою перевірки повноти та достатності реалізованих заходів із захисту інформації на ОІД, атестації комплексу ТЗІ, а також вимоги до розроблення висновків за результатами випробувань та їх програм і методик.

2.2 Бази даних

База даних – сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами; ця сукупність підтримує щонайменше одну з областей застосування. В загальному випадку база даних містить схеми, таблиці, подання, збережені процедури та інші об'єкти. Дані у базі організовують відповідно до моделі організації даних. Таким чином, сучасна база даних, крім самих даних, містить їх опис та може містити засоби для їх обробки [24].

В загальному випадку базою даних можна вважати будь-який впорядкований набір даних. Наприклад, паперову картотеку з формулярами про працівників підприємства у відділі кадрів. Але дана стаття зосереджена на використанні баз даних в інформаційних системах. На даний час застосунки для роботи з базами даних є одними з найпоширеніших прикладних програм.

У сучасних інформаційних системах для забезпечення роботи з базами даних використовують системи керування базами даних. Система керування базами даних — це система, заснована на програмних та технічних засобах, яка забезпечує визначення, створення, маніпулювання, контроль, керування та використання баз даних. Застосунки для роботи з базою даних можуть бути частиною СКБД або автономними.

Через тісний зв'язок баз даних з СКБД під терміном «база даних» інколи необґрунтовано та неточно мають на увазі систему керування базами даних. Але варто розрізняти базу даних — сховище даних, та СКБД — засоби для роботи з базою даних. СКБД з інформаційної системи може бути видалена, але база даних продовжить існувати. І навпаки: СКБД може функціонувати без жодної бази даних [24].

В загальному базу даних неможливо просто перемістити з однієї СКБД до іншої. Але СКБД використовують стандарти, які уніфікують ряд операцій по роботі з даними і дозволяють різним застосункам працювати з базами даних різних СКБД. СКБД часто класифікують за моделлю організації даних. Найвживаніші СКБД використовують реляційну модель, у якій дані подають у виді таблиць. Для кінцевого користувача (та прикладних програм) робота з базою даних напряму неможлива. Всі маніпуляції над даними здійснюють через спеціальні запити, які

надсилають до СКБД. СКБД опрацьовує їх і повертає результат. Безпосередньо з базою даних працює виключно СКБД.

Сучасні СКБД забезпечують функції щодо керування даними, які можна поділити на такі групи [24]:

1) оголошення даних — створення, зміна та видалення визначень, які описують організацію даних;

2) модифікація даних — додавання даних, їх редагування та видалення;

3) отримання даних — надання даних за запитом застосунку у формі, яка дозволяє їх безпосереднє використання. Дані можуть надаватись або у формі, в якій вони зберігаються у базі даних, або в іншій формі (наприклад, через поєднання різних даних);

4) адміністрування даних — реєстрування та відслідковування дій користувачів, дотримання безпеки роботи з даними, забезпечення надійності та цілісності даних, моніторинг продуктивності, резервне копіювання та відновлення даних тощо.

Первинним призначенням бази даних є зберігання масивів даних. Але їх широко використовують і для збереження адміністративної інформації та спеціалізованих даних, наприклад, для інженерних даних чи для економічних моделей. Прикладами використання баз даних можуть бути [24]:

- автоматизовані системи обліку;
- реєстри та каталоги;
- геоінформаційні системи;
- лінгвістичні бази даних, тобто машинні словники різного типу і призначення;
- бази даних транспортних систем;
- системи керування вмістом Інтернет-сайтів, які зберігають у базах даних інформацію про web-сторінки сайту.

Бази даних класифікують за різними критеріями.

За моделлю організації даних розрізняють такі бази даних:

- ієрархічна. Ієрархічна база даних може бути представлена як дерево, що складається з об'єктів різних рівнів. Між об'єктами існують зв'язки типу «предок-нащадок». При цьому можлива ситуація, коли об'єкт не має нащадків або має їх декілька, тоді як у об'єкта-нащадка обов'язково тільки один предок.

– мережна. Така база даних подібна до ієрархічної, за винятком того, що кожен об'єкт може мати більше одного предка.

– реляційна. Реляційна база даних зберігає дані у вигляді таблиць. Найвживаніші СКБД використовують реляційну модель даних.

– об'єктно-орієнтована. У базі даних цього виду дані оформляють у вигляді моделей об'єктів.

За розміщенням даних виділяють такі види баз:

– локальна, або централізована. Така база даних підтримується на одному комп'ютері.

– розподілена. Частини такої бази даних розміщують на різних комп'ютерах мережі.

За технологією фізичного зберігання виділяють:

– БД у вторинній пам'яті (традиційні).

– БД в оперативній пам'яті (in-memory database).

– БД у третинній пам'яті (tertiary database).

2.3 Вихідна документація

Вихідний документ - документ, створений на даному підприємстві і відправлений адресату, копія якого, як правило, залишається у справі.

Вихідні документи оформляються в двох примірниках, крім факсів і телефонограм, який складають в одному примірнику.

Вихідні документи надходять від виконавця керівнику, іноді піддаються процедурі виправлення. Остаточний варіант оформляється згідно з правилами діловодства для додання йому відповідного статусу, реєструється, потім відправляється адресату по каналах зв'язку.

Вихідний документ - документ, відправлений з установи.

Вихідні документи підписуються керівництвом установи або керівниками структурних підрозділів.

Вихідні документи та в необхідних випадках внутрішні документи друкуються на бланках, зберігання яких повинно відповідати порядку зберігання бланків звітності.

Вихідні документи оформляються в двох примірниках, крім факсів і телефонограм, який складають в одному примірнику.

Вихідні документи машинного представлення в заданому форматі представлення розсилаються одержувачам за допомогою стандартних інформаційних технологій. Для розсилки може використовуватися: кур'єрська зв'язок (передача друкованих копій документів або машинних носіїв), електронна пошта, Web-публікації.

Усі вихідні документи реєструються в Журналі вихідної кореспонденції.

Якщо вихідний документ є відповіддю на раніше надійшов документ, то в реєстраційно-контрольній картці на цей документ робиться відповідний запис, в якій містяться номер, дата вихідного документа в прізвище його підписала особи. На ініціативний вихідний документ складається реєстраційно-контрольна картка в кількості примірників, передбаченому діючої в даній організації інструкцією з діловодства. На базі цих карток складається і ведеться обліково-контрольна картотека.

Проект вихідного документа становить виконавець, правильність його оформлення перевіряє секретар. Вихідні документи оформляються в двох примірниках, крім факсів і телефонограм, який складають в одному примірнику. Таке узгодження оформляється візою. Підготовлений проект вихідного документа подається на підпис керівнику. Разом з ним можуть бути представлені й інші документи, на підставі яких був складений проект вихідного документа.

2.4 Технічна документація

Технічна документація – набір документів, що використовуються при проектуванні (конструюванні), створенні (виготовленні) і використанні (експлуатації) будь-яких технічних об’єктів: приміщень, споруд, промислових товарів, програмного та апаратного забезпечення [24].

Технічна документація – комерційні документи, які потрібні при постачанні обладнання та технічних користувальницьких товарів тривалого користування.

До технічної документації відносяться: паспорти, формуляри та описи виробів, інструкції по монтажу та експлуатації, настанови з експлуатації, різні схеми, креслення, відомості про запасні частини інструмента, технічні умови, технічні описи, пояснювальні записки та ін. Технічна документація розробляється на мові країни покупця або на іншій мові по вказівці покупця.

Технічна документація поділяється на такі види:

Конструкторська документація:

- експлуатаційна документація;
- ремонтна документація.

Технологічна документація:

- документи, що визначають технологічний цикл виробу;
- документи, що дають необхідну інформацію для організації виробництва і ремонту виробу.

Конструкторська документація – сукупність конструкторських документів, які залежно від їх призначення містять дані, що потрібні для проектування, виготовлення, контролю, приймання, постачання, експлуатації та ремонту виробу [24].

Конструкторські документи в залежності від представленої в них інформації поділяються на графічні та текстові.

В графічному конструкторському документі основна інформація про технічний предмет представлена у вигляді графічного зображення, що виконане чорним кольором за допомогою ліній, штрихів та крапок. Інформація про предмет у вигляді графічного зображення найбільш зручна при розгляданні пристрою та принципу дії виробу, взаємного розміщення його складових частин, геометричної форми деталей. Часто графічна інформація супроводжується текстовою або знаковою інформацією.

До графічних конструкторських документів належать кресленики та схеми.

Кресленик – документ, який містить зображення технічного предмету або його складової частини та інші дані, що пояснюють функціональне значення предмету та дозволяє його виготовити.

Схема – документ, який містить умовні графічні зображення складових частин технічного предмету та зв’язки між складовими частинами.

Текстові конструкторські документи містять мовну описову інформацію, а також розрахунки та їх результати. Текстовий документ оформляється у вигляді суцільного тексту (технічні умови, технічні описи, пояснювальні записки) або тексту, що розбитий на графи (специфікації, відомості, таблиці і т.д.).

Існує декілька державних стандартів, які визначають правила оформлення технічної документації. Основним серед них являється Єдина система конструкторської документації, що містить положення по виконанні та оформленні

документів, розробці конструкторських документів на вироби та правила виконання і оформлення експлуатаційної та ремонтної документації.

Єдина система конструкторської документації – комплекс державних стандартів, що встановлюють взаємозв'язані оптимальні правила, вимоги і норми по виконанню, оформленню конструкторської документації, яка розробляється і застосовується на всіх стадіях життєвого циклу виробу (при проектуванні, виготовленні, контролі, експлуатації, ремонті, утилізації).

У документах про технічний захист інформації одночасно використовуються такі терміни та визначення:

Засіб технічного захисту інформації від НСД – це програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну програмну та/або конструкторську документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз НСД для інформації в КС, або використовується для контролю ефективності захисту інформації від НСД в таких системах [24].

Захищений від НСД компонент обчислювальної системи - це програмний, апаратний або програмно-апаратний засіб у якому додатково до основного призначення передбачено функції захисту інформації від загроз НСД.

Впровадження засобу ТЗІ – встановлення, монтаж, налагодження та участь в дослідній експлуатації засобу ТЗІ в КС.

Впроваджувальні організації – суб'єкти господарської діяльності, які здійснюють впровадження засобів ТЗІ.

Супроводження засобу ТЗІ – діяльність розробника (впроваджувальної організації) з надання послуг, необхідних для забезпечення функціонування засобу ТЗІ впродовж його життєвого циклу.

Договір на супроводження – документ, який засвідчує взаємні зобов'язання розробника (впроваджувальної організації) і користувача щодо супроводження засобу ТЗІ під час його експлуатації.

Згідно з Положенням про технічний захист інформації в Україні в КС, де обробляється інформація, яка належить до державних інформаційних ресурсів, або інформація, вимога щодо захисту якої встановлена законом, повинні використовуватись засоби ТЗІ, які мають документ, що засвідчує їх відповідність вимогам нормативних документів з питань технічного захисту інформації.

Склад засобів ТЗІ, що використовуються під час створення комплексу засобів захисту (КЗЗ) інформації, визначають власники КС, де обробляється інформація, яка підлягає захисту, або уповноважені ними суб’єкти системи ТЗІ, з урахуванням того, що ці засоби повинні мати рівень гарантій коректності реалізації послуг безпеки (НД ТЗІ 2.5-004-99) не нижчий від рівня гарантій створюваного КЗЗ.

Дозволяється в АС класів "1" та "2" (НД ТЗІ 2.5-005-99) використання засобів ТЗІ з рівнем гарантій на один нижче від рівня гарантій створюваного КЗЗ, за умов реалізації в цих АС необхідного обсягу організаційних заходів. Обсяг цих заходів визначається моделями загроз та порушника, умовами експлуатації АС тощо.

Засоби криптографічних перетворень, які є складовою частиною засобів ТЗІ, повинні відповідати вимогам нормативних документів з питань криптографічного захисту інформації.

3 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ EIP ВІД DDOS АТАК

Зараз у всьому світі жодна країна не застрахована від нападу на електронні інформаційні ресурси. Наприклад у 2016 році Система захищеного доступу до мережі Інтернет Державного центру кіберзахисту зафіксувала та відбила декілька DDoS-атак, які були спрямовані на порушення доступності сайтів органів державної влади України. Про це повідомляє Держспецзв'язку.

За словами фахівців, атаки відбувалися з великої кількості заражених хостів ботнетів, які маскувались під легальний трафік. Її особливістю було те, що поряд з DDoS-атакою відбувалася також атака ботів, яка імітувала поведінку користувачів. Зловмисники проводили атаку у два етапи.

Здебільшого вона відбувалася за допомогою VPN-трафіку, маскуючись під різні країни, зокрема й Україну. Однак атаки вдалося зафіксувати та успішно відбити. Доступу до сайтів порушено не було.

У наші дні всі компанії, що мають зв’язок із забезпеченням інформаційної безпеки та протидії кібератакам, помітили великий зріст кількості DDoS-атак і їх потужність.

DDoS-атака – комплекс дій, здатний повністю або частково вивести з ладу інтернет-ресурс. В якості жертви може виступати практично будь-який інтернет-ресурс, наприклад веб-сайт, ігровий сервер або державний ресурс. На даний момент практично неможлива ситуація, коли хакер поодинці організовує DDoS-атаку. У більшості випадків зловмисник використовує мережу з комп’ютерів, заражених вірусом. Вірус дозволяє отримувати необхідний і достатній віддалений доступ до зараженого комп’ютера.

Дуже часто можна почути про неефективність засобів захисту та протидії цим атакам, бо періодично ми чуємо повідомлення в засобах масової інформації про недоступність тих чи інших ресурсів у результаті розподілених атак, спрямованих саме на відмову в обслуговуванні. Також у наш час атаки вже ведуться не тільки на величезні компанії, але і на невеликі сайти, які раніше не піддавалися таким атакам і увазі зловмисників. Тому у даний час ці невеликі, через їх затребуваність, проблеми з їх роботою можуть бути дуже критичними для нас. Тобто мотиви, які рухають зловмисниками, повністю змінились. Якщо раніше DDoS-атаки визивались заради протестів або хуліганства, то сьогодні вони вже все

частіше використовуються для шантажу або як спосіб вимагання грошей. Тобто DDoS-атаки переросли з одиночних протестних акцій вже у великий кримінальний бізнес, який не обмежується тільки вимаганням грошей, але й інструментом терористичних операцій. Зараз у всьому світі дуже часто відбуваються атаки на сайти державної влади напередодні будь-яких великих подій, які пов’язані з інтернет ресурсами.

Якщо визвати відмову у роботі великого ресурсу, який має у своєму арсеналі активні засоби протидії, можна зробити тільки з допомогою заповнення всієї полоси пропускання каналу зв’язку, що надає причину для створення та підтримки великої бот-мережі. У цей же час для паралізації невеликого регіонального ресурсу для котрого буде достатньо досить невеликої по потужності атаки і як наслідок з цього, використання невеликої бот мережі. Оскільки обслуговування та підтримка таких бот-мереж є менш витратним, і потенційно такі бот-мережі може зробити більша кількість зловмисників. Цей факт на тлі відсутності адекватних засобів протидії робить загрози безпеки регіональних ресурсів в результаті DDoS-атак особливо значущим. З одного боку, для протидії таким атакам можуть бути ефективно застосовані засоби, призначені для відбивання великих атак. З іншого - впровадження і підтримка таких коштів економічно затратно і не по кишені регіональних ресурсів. Засоби протидії, спеціалізовані саме на забезпечення безпеки невеликих і середніх ресурсів, отримали менший розвиток через переважання в минулому саме великих атак. І в даний час відстають від еволюції самих DDoS-атак.

3.1 Огляд сучасних DDoS-атак

Спочатку нам потрібно з’ясувати, чим є DDoS-атака. Відповідно це розподілена атака відмови в обслуговуванні, вона є спробою порушення нормального трафіку цільового сервера, послуги або мережі, завдяки переповненню цілі або оточення її інфраструктури потоком інтернет-трафіку. Також DDoS-атаки набувають ефективності за допомогою використання певної кількості скомпрометованих комп’ютерних систем як джерел трафіку. Тобто якщо подивитись з іншого боку, це схоже на несподіваний затор, що забиває шосе, заважаючи звичайному пересуванні потраплять до місця призначення.

У DDoS-атаці в ролі атакуючого виступає бот-мережа. Вона навіть іноді може налічувати до тисячі хостів. Частіше за все це звичайні комп’ютери, які були заражені шкідливим ПЗ. Саме ці програми, які зазвичай працюють у фоновому режимі, посилають запити, котрі й виводять сервер з ладу. Тобто коли бот-мережа націлена на сервер або мережу жертви, кожен бот надсилає запити на IP-адресу цілі, відповідно саме це і призводить до відмови в обслуговуванні звичайного трафіку. Через те, що кожен бот є цілком законним Інтернет-пристроєм, розрізнити трафік атаки від повсякденного трафіку іноді буває дуже складно. На рисунку 3.1 [1] показано приклад простішої заказної DDoS програми.

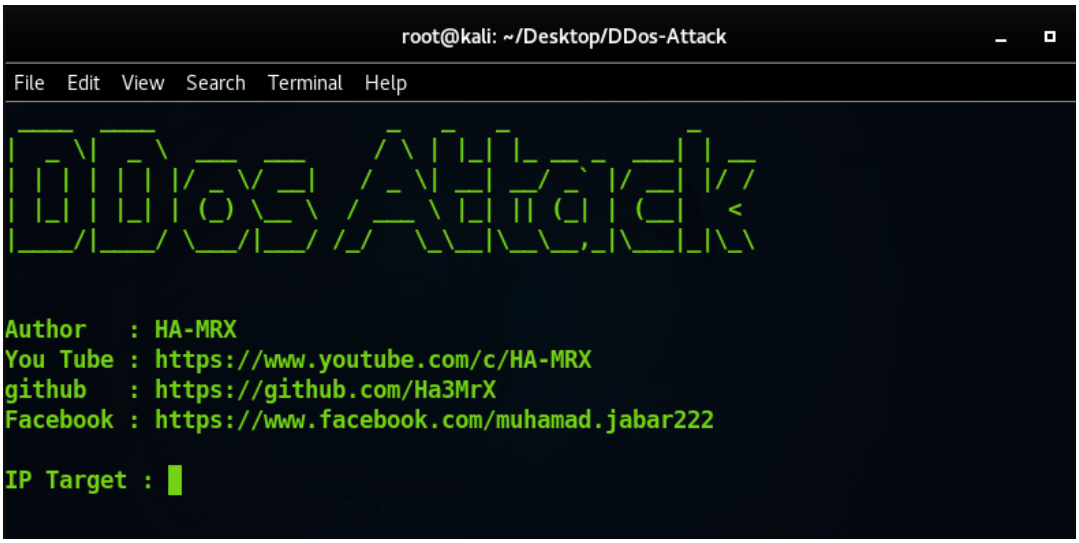

Рисунок 3.1 – DDoS програма

Велика кількість DDoS-атак націлена саме на пропускну здатність мережі, тобто на її перенавантаження. Пропускна здатність відображає обсяг даних, переданих мережею чи її частиною за одиницю часу.

Пропускну здатність можна вимірювати між будь-якими двома вузлами або точками мережі, наприклад між клієнтським комп'ютером і сервером, між вхідним і вихідним портами маршрутизатора. Для аналізу і настройки мережі дуже корисно знати дані про пропускну здатність окремих елементів мережі.

Важливо відзначити, що через послідовний характер передачі пакетів різними елементами мережі загальна пропускна здатність мережі будь-якого складеного шляху в мережі буде дорівнює мінімальній з пропускних здатностей складових елементів маршруту. Для підвищення пропускної здатності складеного шляху необхідно в першу чергу звернути увагу на самі повільні елементи - в даному

випадку таким елементом, швидше за все, буде маршрутизатор. Слід підкреслити, що якщо переданий по складеному шляху трафік буде мати середню інтенсивність, перевершуючи середню пропускну здатність самого повільного елемента шляху, то черга пакетів до цього елемента буде рости теоретично до нескінченності, а практично - до тих пір, поки не заповниться його буферна пам'ять, а потім пакети просто почнуть відкидатися і втрачатися.

Іноді корисно оперувати з загальною пропускною здатністю мережі, яка визначається як середня кількість інформації, переданої між всіма вузлами мережі в одиницю часу. Цей показник характеризує якість мережі в цілому, не диференціюючи його по окремих сегментах або пристроях.

Зазвичай при визначенні пропускної здатності сегмента або пристрою в даних не виділяються пакети якогось певного користувача, додатки або комп'ютера - підраховується загальний обсяг переданої інформації. Проте для більш точної оцінки якості обслуговування така деталізація бажана, і останнім часом системи управління мережами все частіше дозволяють її виконувати.

3.2 Види DDoS-атак

Попри те, що DDoS-атака пропонує менш складний режим атаки, ніж інші форми кібератак, вони стають все сильнішими та витонченішими. Існує три основні категорії нападів.

1) атаки на основі обсягу або об’ємні атаки, вони використовують великий трафік для заповнення пропускної здатності мережі;

2) атаки протоколів, вони зосереджені на використанні ресурсів сервера;

3) атака на програми, які зосереджені на веб-додатках і вважаються найскладнішим і найсерйознішим видом атак.

Об’ємні атаки розподіленої відмови в обслуговуванні відрізняються від інших двох типів DDoS-атак - протокольних DDoS-атак та DDoS-атак на рівні додатку, - оскільки вони засновані на методах грубої сили, які заповнюють ціль пакетами даних для споживання пропускної здатності та ресурсів . Два інших типи атак, як правило, використовують значно меншу пропускну здатність, а також більше зосереджені на конкретних аспектах своїх цілей, таких як конкретний протокол чи послуга.

Зазвичай хакери запускають об’ємні DDoS-атаки, використовуючи бот-мережі . Ці атаки часто використовуються спільно з іншими типами DDoS-атак як прикриття для інших методів злому, таких як спроби проникнення, які максимально ускладнюють моніторинг безпеки веб-додатків. Ці атаки також можуть бути використані для вимкнення інфраструктури безпеки жертви, пригнічуючи її та створюючи шлях для інших атак.

Ці атаки працюють, щоб залити ціль в надії сповільнити або зупинити їх послуги. Зазвичай розміри запитів складають 100 Гбіт / с; проте останні атаки збільшились до 1 Тбіт / с.

Об’ємні атаки поширені через нижчий технічний бар’єр для генерації великого обсягу запитів. У більшості випадків хакери використовують прості прийоми посилення для масштабування своєї атаки. На рисунку 3.2 наведено приклад, як виглядає цей тип атака на графіку.

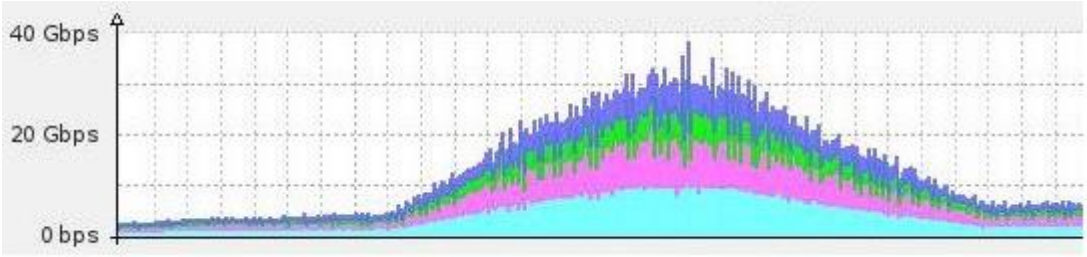

Рисунок 3.2 – Графічний вигляд об’ємної DDoS-атаки

Також існують об’ємні атаки, що використовують відбивні прийоми.

Відбивні атаки - це ті, які мають найбільший вплив на пропускну здатність. Під час відбивної атаки зловмисник надсилає невеликі запити до ряду законних служб, розміщених в Інтернеті. Їхній один ключовий фокус - вони роблять вигляд, що запит надійшов від жертви, і вони використовують запит, який викликає велику відповідь. В результаті вони відправляють потік невеликих запитів до служб в Інтернеті, таких як domain name system і network time protocol, а потім, у свою чергу, ці служби надсилають великі відповіді жертві. Перетворення малих запитів у великі відповіді - ось чому це називається посиленням.

Наприклад, така атака, як пінг-наводки, вона вдає із себе підроблені пінг-пакети з величезного набору вихідних IP-адрес, що заповнюють сервер. У ході цієї атаки кіберзлочинець настільки заливає сервер, що він переходить до автономного

режиму. Цю атаку дуже важко виявити, бо вона дуже схожа на звичайний трафік, який поступаю до сервера.

Відповідно DDoS-атаки на основі протоколу використовують слабкі місця в стеках протоколів. Цей тип атак споживає серверні ресурси або будь-яке інше мережеве обладнання в середині обробних потужностей. Результатом є порушення роботи служби. Ці атаки у першу чергу шукають можливість використати ваш мережний стек, надіславши велику кількість пакетів, яку не може обробити сервер, або більшу пропускну здатність, ніж те, що можуть обробити ваші мережеві порти.

Наприклад, така атака, як SYN повінь, у ході цієї атака зловмисники використовують слабкі сторони тристороннього рукостискання підключення протоколу управління передачею, що є процесом комунікації між клієнтом, хостом і сервером. Зловмисники відправляють SYN-пакети на цільовий сервер у вигляді підробленого повідомлення, поки з'єднання з сервером табличної пам'яті не вичерпається, в результаті чого вся служба буде вимкнена [4].

В основі атаки на програми, лежить атака на веб-сервери. Однак атаки на рівні додатків розвиваються на таких платформах, як WordPress, Joomla, Magento та інших. Ціль атаки на рівні додатків є видалення програми, Інтернет-служби або веб-сайту.

Зазвичай ці атаки менші за ті що ми бачили раніше. Але наслідки від цих атак можуть бути дуже неприємними, оскільки вони можуть залишатися непоміченими. Ось чому їх називають «низькими і повільними атаками» або навіть «атаками з повільною швидкістю». Вони можуть бути тихими і незначними, особливо якщо порівнювати їх із загально мережними атаками, але вони можуть бути досить руйнівними.

3.3 DDoS-атаки націлені на конкретні протоколи

На відміну від нападів розподіленої відмови в обслуговуванні на рівні додатків та об'ємних DDoS-атак, протоколи DDoS-атак покладаються на слабкість протоколів Інтернет-зв'язку. Оскільки багато з цих протоколів використовуються у всьому світі, зміна їх роботи є складною і дуже повільною для розгортання. Що більше, для багатьох протоколів властива їм складність означає, що навіть коли їх переробляють для виправлення наявних недоліків, часто вводяться нові слабкі місця, що дозволяють застосовувати нові типи атак протоколів та мережевих атак.

Велика кількість DDoS-атак використовують вразливості в основному протоколів Internet, а саме TCP/IP. Тобто його спосіб обробки системами запитів SYN.

TCP – це протокол контролю передачі даних у комп’ютерної мережі. TCP обгортає кожен пакет даних заголовком, що містить 10 обов’язкових полів на загальну суму від 20 до 60 байт, 40 байтів для параметрів. Кожен заголовок містить інформацію про з'єднання та поточні дані, що надсилаються.

Поля заголовка TCP:

1) порт джерела – порт пристрою, що надсилає;

2) порт призначення – порт приймального пристрою;

3) порядковий номер – пристрій, що ініціює з’єднання TCP, повинен вибрати випадковий початковий номер послідовності, який потім збільшується відповідно до кількості переданих байтів;

4) номер підтвердження – приймаючий пристрій підтримує номер підтвердження, починаючи з нуля. Він збільшує це число відповідно до кількості отриманих байтів;

5) зміщення даних TCP – визначає розмір заголовка TCP, виражений 32-розрядними словами. Одне слово позначає чотири байти;

6) зарезервовані дані – зарезервоване поле завжди встановлюється на нуль;

7) прапор керування – TCP використовує дев’ять прапорів управління потоками;

8) контроль сума TCP розміру вікна – відправник генерує контроль суму і передає її в кожному заголовку пакету. Ця сума може використовуватися для перевірки помилок у отриманому заголовку та корисному навантаженні;

9) терміновий покажчик – вказує зміщення байтів від поточного порядкового номера байту до місця розташування термінових даних;

10) параметри – це поля для встановлення максимальних розмірів сегментів, вибіркових підтверджень та увімкнення масштабування вікон для більш ефективного використання мереж із високою пропускною здатністю.

DDoS-атаки, які використовують цей протокол, націлені саме на особливість його механізму синхронізації – триетапне рукостискання, приклад цього механізму наведено на рисунку 3.3 [20].

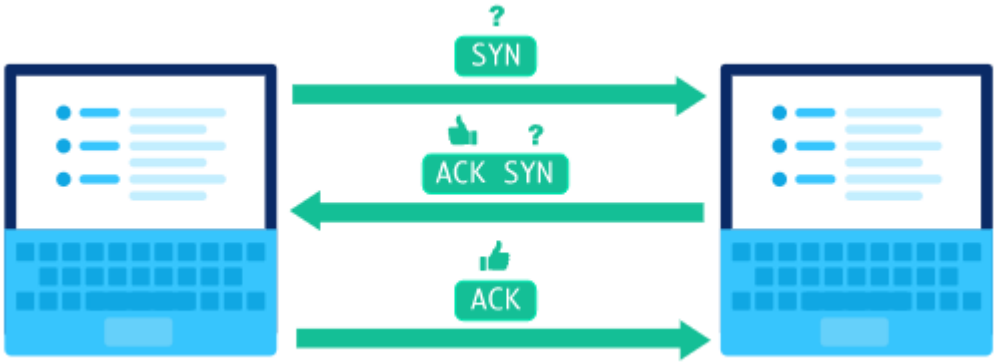

Рисунок 3.3 – Триетапне рукостискання

Спочатку клієнт відправляє серверу команду SYN, на що сервер відповідає SYN-ACK, потім клієнт відповідає своїм ACK і з'єднання встановлюється. При SYN-флуд нападник або не посилає очікуваного ACK і продовжує надсилати SYN, збільшуючи кількість «напіввідкритих» з'єднань, або відправляє серверу фальсифікований IP, куди і йдуть SYN-ACK. При цьому, оскільки з того IP команди SYN не правили, то й ACK не зробить. Через деякий час весь канал виявляється забитий. Тобто у цьому випадку зловмисники використовують вразливість TCP протоколу, а саме, відсутність механізму перевірки заповнення службових заголовків пакету. Приклад роботи цього типу атака, наведено на рис. 3.4.

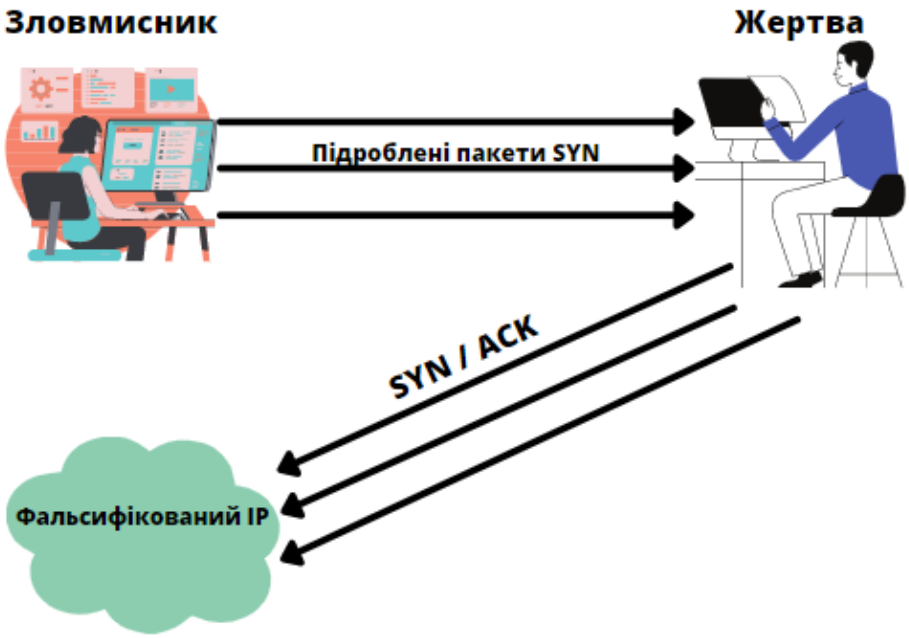

Рисунок 3.4 – SYN-flood атака

Існують атаки на рівні протоколу UDP, цей протокол використовуються зловмисником, через те що він не має механізму запобігання перевантажень буфера.

Велику роль грає, яка версію протоколів використовується. Наприклад, якщо ваша мережа використовую не оновлену версію протоколу мережевого часу, який призначений для синхронізації внутрішнього годинника пристроїв, підключених до інтернету, і виконує важливу функцію в архітектурі інтернету. У старих версіях цього протоколу, увімкнена за замовчуванням опція monlist. Атака на цей протокол заснована на опції monlist, цей запит отримує список останніх 600 клієнтів, які користувалися сервісом, саме це і використовує зловмисник, для завдавання мережі, яка використовує цей протокол. Вони розсилають пакети з запитами, а в якості джерела при формуванні запита вказують IP-адреса жертви. Оскільки network time protocol – це UDP протокол, то сервер без перевірки відправляє відповідь тому, хто його запитував. Через те, що відповідь, яку відправляє сервер, значно перевищує запити, що призводить до завантаженості каналу зв’язку і викликає нездатність сервера відповідати на легітимні запити користувачів.

3.4 Методи захисту від DDoS-атак

Існує дві групи методів боротьби з DDoS-атаками. Перша групи, це методи, що спрямовані на запобігання самого факту атаки й друга група, це методи, які використовуються вже після початку атаки, тобто це методи активної протидії та пом’якшення самого результату та впливу від цієї атаки. До способів запобігання нападів можуть бути віднесені законодавчо-правові заходи. Наприклад, неприпустимість участі в конфліктних ситуаціях, або заходи, що використовуються для усунення наслідків, яких хоче досягти злочинець, таких як виявлення та приховування критичних ресурсів. Також на цьому етапі усуваються уразливості та оновлюється відповідне апаратне та програмне забезпечення.

Існує кілька досить простих технічних заходів для часткового зниження ефективності атаки, особливо на її початку:

– потрібно обмежити пропускну здатність вашого маршрутизатора для запобігання перевантаження сервера;

– додавання фільтрів, які відхиляють атакуючі адреси;

– налаштування тайм-ауту напіввідкритих з’єднань;

– відхилення підроблених і спотворених пакетів.

Кілька типів мережних атак призначені для використання різних типів вразливостей. Це можуть бути вразливості у програмному забезпеченні серверу. Або завади, пов’язані з використанням не вдосконалених програмних скриптів, які можуть надмірно витрачати ресурси сервера. У цьому випадку для того, щоб досягти бажаного ефекту, зловмиснику потрібно організувати менш потужну атаку.

Тобто з самого початку створення свого серверу нам необхідно зрозуміти, яку пропускну здатність потребує мережа, для цього потрібно обміркувати такі пункти:

– які програми будуть використовуватися;

– вимоги до пропускної здатності кожного додатку;

– помножити вимоги програм на кількість очікуваних одночасних користувачів.

Також існує можливість підключення додаткових каналів зв’язку, навіть якщо після підрахування необхідної пропускної здатності показує, що вони не потрібні. В такому випадку є можливість без наслідків подолати несподівані стрибки трафіку. При реалізації DDoS-атаки, ці канали не врятують мережу, але вони дадуть кілька додаткових хвилин для прийняття активних заходів, щодо протидії цим атакам.

Після того, як атака вже почалась, потрібно вже розглядати активні заходи, що спрямовані на протидію атаки. Найважливішим з цих заходів є нарощування ресурсів та фільтрація трафіку.

Перед тим як почати нарощування ресурсів, необхідно зробити детальний аналіз завантаженості серверу і мережевого сегмента з метою забезпечення вузьких місць. Наприклад, якщо у нормальному режимі сервер використовує значну частину каналу зв’язку, відповідно до цього виходить, що у разі атаки, зловмисник буде намагатись повного заповнення цього каналу шкідливими запитами. У такому випадку потрібно заздалегідь збільшити пропускну здатність цього каналу.

«Вузькі місця», що були виявлені у результаті аналізу, необхідно наділити додатковими ресурсами. Якщо на фізичному сервері основним споживачем ресурсів є сервер баз даних, буде доречно перемістить його на окремо виділений сервер. Якщо продовжувати розглядати веб-сервер, як суб’єкт атаки, то можна помітити, що зайве навантаження може генерувати сам веб-сервер або розміщені

на ньому програмні скрипти. Відповідно у цьому випадку нам необхідно збільшити ресурси самого серверу, а саме: додаткова пам’ять, мабуть, більш потужний процесор тощо. Або використати спеціальні інструменти для налаштування веб-серверів і відділити його в окремий кластер.

Цей підхід зі збільшення не є ідеальним рішенням від мережевих атак, окрім того, він має деякі недоліки:

– цей метод неможливо виконати негайно на початку атаки;

– сама підтримка зайвих ресурсів є економічно недоцільна у період очікування атаки.

Для подолання цих недоліків можна використовувати хмарні технології, які дозволяють збільшувати ресурси тоді, коли це потрібно. Тобто користувачу цієї технології надається необхідна кількість ресурсів у потрібний час. Відповідно, коли мережа з цією технологією отримує збільшення навантаження, тобто кількість шкідливих запитів, у цей час серверу надається необхідна кількість ресурсів, для того, щоб обробити всі запити. В результаті цього сервер продовжує свою роботу. Але є і мінуси у цього методу, тому що клієнту потрібно буде оплачувати додаткові потужності, тобто платити за обробки шкідливих запитів.

Переваги хмарових технологій перед іншими:

– власнику серверу не потрібно наймати та навчати додатковий персонал;

– висока місткість фільтрації;

– велика швидкість підключення;

– можливість використати пробний період.

Інший спосіб нарощування ресурсів серверу, надає нам можливість нарощувати ресурси в мережі доставки контенту. В цьому випадку відбувається кешування складових веб-сервера і доставка цього кешу через розподілену мережу вузлів. Також при виборі оптимального курсу, враховується географічне положення, тобто обирається найближчий вузол до сервера. Відповідно, коли відбувається атака і шкідливий трафік попадає до мережі, він поділяється між різними вузлами й втрачає свою потужність, або є варіант коли цей трафік, навіть не попаде до потрібного вузла.

У будь-якому випадку всі ці методи не є цілком безпечними, тому що через них потрібна обробка всіх запитів без будь-якого виключення.

Будувати захист від DDoS-атак необхідно роботи на всіх рівнях. Наприклад, для забезпечення доступності сайту, трафік потрібно пропускати через мережу очищення, організовувати захист сайту на транспортному і мережевому рівнях, де саме буде відбуватися фільтрація і аналіз трафіку, який поступає на сервер.

Тому наступна група методів, спрямована на запобігання атак, а саме фільтрація трафіку. Тобто йдеться про блокування шкідливих запитів.

Для ефективних заходів щодо протидії та фільтрації трафіку необхідне вирішення двох тісно пов'язаних проблем. Перше завдання пов'язане з виявленням факту про початок атаки, друге – з визначенням джерела атаки. Чим точніше вирішуються ці завдання, тим більші заходи протидії будуть ефективнішими. На сьогодні існує два методи визначення початку атаки. Це підхід, заснований на аналізі зловживань, та підхід оснований на аналізі аномалій. У першому підході виявлення атаки відбувається шляхом порівняння даних, що характеризують поточні стан системи, з даними, характерними для типових атак. Другий підхід оцінює поточний стан системи з її нормальним станом. Обидва ці підходи мають свої мінуси, так, наприклад, перший підхід може бути не ефективним при виявленні принципово нових типів атак. Це особливо актуально в контексті саме DDoS-атак, оскільки зловмисники намагаються перейти від аномального поведінки і симулювати дії реальних користувачів. для успішної експлуатації другого підходу необхідно накопичення статистичних даних, що свідчать про нормальне функціонування системи. Отже, для побудови ефективної системи виявлення доцільно використовувати обидва ці підходи [12].

Тобто, коли вся ця система працює, буде відбуватися постійний сбір даних, які показують стан системи. Після цього відбуватиметься обробка та аналіз на предмет відмінності від модельних даних. І якщо атака починається, свою роботу починають механізми виявлення джерела трафіку, а далі проводиться порівняння з модельними даними. Порівняння може відбуватися різними методами.

Найефективніша фільтрація трафіку – це фільтрація підозрілої мережевої активності на рівні хостингу або інтернет-провайдеру. Також це можна виконувати різними методами, тобто засобами мережевих маршрутизаторів та за допомогою спеціального обладнання.

Власник же сайту, веб-сервісу або іншого мережевого проекту, зі свого боку, для мінімізації ризиків і втрат від DDoS повинен [13]:

1) ретельно обстежити логіку свого продукту: ще на етапі розробки і

тестування можна виключити помилки і уразливості;

2) вести контроль версій ПЗ і мережевих служб: необхідно своєчасно оновлювати програмне забезпечення мережевих служб. Також потрібно підтримувати код самого продукту в актуальному і стабільному стані. Рекомендується навіть розгортати проект на декількох серверах - продуктовому, тестовому і бекап-сервері. Також рекомендується використовувати системи контролю версій для можливості відкату проекту до попередньої стабільної збірці;

3) стежити за доступом до мережних служб: делегування прав на операції вимагає опрацювання. Необхідно забезпечити кілька рівнів доступу. До мережних служб сервера і архіву версій проекту. Список осіб, які мають доступ до ресурсів сервера, необхідно підтримувати в актуальному стані - наприклад, своєчасно відключати доступ звільнилися співробітникам. Також потрібно скидати паролі і облікові записи при будь-якій підозрі на компрометацію;

4) контролювати панель адміністратора: рекомендується обмежити доступ до панелі внутрішньої, або VPN-мережею;

5) сканувати систему на наявність вразливостей: в цьому допоможуть публічні рейтинги, або інструменти розробника;

6) використовувати брандмауер додатків: автоматизуйте перевірку мережевого трафіку і валідації запитів до портів і служб сервера;

7) розподіляти трафік за допомогою CDN: за рахунок розподіленого зберігання контенту навантаження на ресурси сервера оптимізується, що прискорює обробку трафіку і запитів;

8) вести списки контролю доступу: для персонального обмеження доступу до мережевих вузлів;

9) очищати кеш DNS: для захисту від спуфинга;

10) використовувати захист від спаму: один з джерел вразливостей - форми зворотного зв’язку. Зловмисники можуть направити своїх ботів масово заповнювати їх відправляти однотипні дані на сервер;

11) використовувати контратаку: шкідливий трафік можна перенаправити на мережу атакуючого. В результаті це не тільки збереже доступність Вашого сервера, але і тимчасово виведе зловмисника з гри;

12) використовувати розподілене зберігання і бекапіроване: в разі відмови одного або декількох серверів Вашої мережі Ви зможете відновити роботу ресурсу на іншій машині. До цього часу там вже буде розгорнута функціональна копія

Вашого проекту.

13) використовувати апаратні засоби захисту від DDoS;

14) ретельно вибирати хостинг-провайдера: необхідно вибирати постачальника, що дає гарантії захисту від усіх сучасних загроз. Також важливо мати цілодобову лінію підтримки, панель адміністратора з необхідними інструментами аналітики за конкурентними умовами.

Найбільша складність при захисті від DDoS-атак є підроблені IP-адреси для атакуючих пристроїв. Цю проблему можна вирішити за допомогою технології вихідної фільтрації. Тобто ця технологія спрямована на граничний маршрутизатор, який стоїть перед магістральним маршрутизатором. Також ці маршрутизатори повинні мати адреси всіх пристроїв, що входять до цієї системи. Через це всі підроблені пакети відкидаються, ще до їх попадання у мережу. Це скоротить процес ідентифікації в дослідженні DDoS-атак.

Також завжди потрібно пам’ятати про захист від атак на рівні додатків. Ці атака ефективні, бо витрачають дуже мало ресурсів для запуску, але для її пом’якшення або зупинки потрібно застосувати велику кількість ресурсів мережі. Ефективність впливу як на цільовий сервер, так і на мережу вимагає меншої загальної пропускної здатності для досягнення того самого руйнівного ефекту; атака на рівні програми створює більший збиток при меншій загальній пропускній здатності.

Розрізнити трафік атак від звичайного трафіку важко, особливо у випадку атаки на рівні програми, наприклад бот-мережі, що виконує атаку HTTP Flood проти сервера жертви. Оскільки кожен бот у бот-мережі робить, здавалося б, законні мережеві запити, трафік не підроблений і може виглядати “нормальним” за своїм початком.

Атаки на рівні додатків вимагають адаптивної стратегії, що включає можливість обмеження трафіку на основі певних наборів правил, які можуть регулярно коливатися. Такі інструменти, як правильно налаштована WAF, можуть зменшити кількість підробленого трафіку, який передається вихідному серверу , значно зменшуючи вплив спроби DDoS.

З іншими атаками, такими як повені SYN або атаками відбиття, такими як посилення NTP , можна використовувати стратегії зменшення трафіку досить ефективно за умови, що сама мережа має пропускну здатність для їх прийому.

Одним із методів є реалізація виклику пристрою, який робить мережний запит, щоб перевірити, чи це бот . Це робиться за допомогою тесту, подібного до тесту CAPTCHA, який зазвичай зустрічається під час створення облікового запису в Інтернеті. Завдяки такому засобу, як обчислювальна задача JavaScript, можна зменшити кількість атак.

Інші шляхи зупинки повені HTTP включають використання брандмауера веб-додатків , управління та фільтрацію трафіку через базу даних про репутацію IP та інтенсивний аналіз мережі інженерами.

3.5 Гібридний захист від DDoS-атак

У наші дні гібридне рішення захисту від DdoS-атак стає дуже популярним, бо воно є дуже ефективним. Тобто у цьому випадку система користувача працює разом із операторським рішення захисту або використовує розподілену мережу. У розподіленої мережі, шкідливий трафік проходить через розподілені центри фільтрації, де і відсікається.

Гібридний підхід, який використовує відбір трафіку на рівні провайдеру для уникнення лавиноподібних атак і рішення для захисту системи, які використовує власник серверу, вважається оптимальним при захисті від DDoS-атак.

Послуги щодо захисту від DDoS надаються операторами зв’язку, провайдерами або іншими захисними компаніями. Вони виконують моніторинг трафіку в реальному часі, для того щоб знайти або засікти аномальний трафік. Також займаються захисними функціями, які дозволяють приховати обладнання клієнта від зловмисників, заборонивши до нього доступ з інтернету, застосовують інтелектуальні системи.

Тобто гібридні захисти є комплексом захисних актів, які складаються з локальних методів захисту та допомоги ззовні. Це можуть бути як хмарні технології, так і надання захисту зі сторонніх ресурсів.

3.6 Web application firewall, як захист від DDoS-атак

У першу чергу потрібно зазначити, чим саме є WAF. Фаєрвол веб-додатків або web application firewall – це сукупність моніторів і фільтрів, що призначені для

виявлення та блокування атак на веб-додаток [15]. WAF належать до прикладного рівня моделі OSI.

Цей фаєрвол увібрав у себе здатність захищати веб-додатки від усіх відомих інформаційних атак. Він використовується як накладний засіб захисту. Тобто, це означає, що він розташовується перед серверів та аналізує трафік, який надходить до нього або який виходить з нього. У режимі реального часу буде прийнято рішення щодо надання або відхилення у доступі.

Основне призначення WAF – захист веб-додатків від несанаційного доступу, навіть у разі наявності критичних вразливостей. Відповідно WAF, захищає веб-програми, фільтруючи, контролюючи та блокуючи будь-який зловмисний трафік HTTP та HTTPS, що поступає до веб-програм. Це відбувається завдяки набору політик, які допомагають визначати, якій трафік шкідливий, а який не несе ніякої шкоди нашому додатку. На рис. 3.5 [14] наведено приклад системи яка використовує цей тип захисту.

Рисунок 3.5 – Захист завдяки Web Application Firewall

WAF може бути представлено у формі програмного забезпечення, приладу або надитися як послуга. Цю політику можна налаштовувати відповідно до потреб серверу.

Цей фаєрвол можна розгорнути в залежності від наших потреб. Тобто цим додатком можна керувати самостійно, або можна передати управління на аутсорс. Також існує спосіб хмарного розгортання, це найшвидший варіант отримання WAF для нашого серверу.

Режими розгортання WAF [14].

1) Хмарно та повністю керований як сервіс - це чудовий варіант, якщо вам потрібен найшвидший і безпроблемний спосіб отримати WAF перед своїми програмами.

2) На основі хмари та самокерування - отримайте всю гнучкість і переносимість політики безпеки в хмарі, зберігаючи при цьому контроль над керуванням трафіком і налаштуваннями політики безпеки.

3) Хмарна та автоматична підготовка - це найпростіший спосіб розпочати роботу з WAF у хмарі, розгортаючи політику безпеки простим та економічно вигідним способом.

4) Локальний розширений WAF - це відповідає найвимогливішим розгортанням, де гнучкість, продуктивність та розширені проблеми безпеки є критично важливими.

Оскільки WAF шукає атаки, які використовуються проти основних функцій програми, він може виявляти не тільки загальні атака, такі як введення SQL та міжсайтовий сценарій, але також може виявляти запити та інші модифіковані або самогенеровані вхідні дані, спрямовані на програму, яка намагається якимось чином обдурити або скомпрометувати програму - кожна з яких знаходиться поза сферою дії рішення щодо пом’якшення атаки DDoS. Нові технології WAF також можуть генерувати відбитки пальців користувачів за тим, як користувачі поводяться під час взаємодії із додатком. Користувачі зловмисних та зловмисних програм, як правило, поводяться послідовно при використанні програми, щоб користувачі могли бути ідентифіковані за тим, як вони рухаються через додаток, і з якими частинами вони взаємодіють. На те, як користувач взаємодіє з додатком, не впливає зміна приналежності домену та IP-адреси користувачів і, отже, не впливає на відбитки пальців [15].

Завдяки технології WAF можна визначати як нормальних користувачів, так і зловмисників. Тобто нормальних користувачів можна ідентифікувати завдяки послідовної поведінки, яка працює з додатком у межах нормальних параметрів, тоді як у зловмисника все буде навпаки. Для того щоб створити ідентифікатор нового пристрою, технологія WAF, збирає велику кількість різних інформаційних точок про пристрій, для того щоб у подальшому цей пристрій мав свій унікальний ідентифікатор. Робота нових пристроїв постійно відстежуються, потім вже класифікуються як нормальний користувач, або як зловмисник.

3.7 Захист протоколів від DDoS-атак

На сьогоднішній день зловмисники навчилися використовувати вразливості протоколів, які використовуються вашою мережею, тому в цьому розділі я наведу приклади захисту від найпопулярніших DDoS-атак.

Існує декілька етапів, які допоможуть частково захиститись від SYN-flood. Ми маємо можливість обмежити розмір пам’яті сервера для кожного вхідного SYN-пакета. Також потрібно використовувати SYN-cookie, тобто використовувати криптографічне хешування. У цьому випадку сервер відправляє SYN-ACK відповідь з номером послідовності, яка складена з IP-адреси клієнта, номера порту і інший унікальної інформації, що ідентифікує клієнта. Коли клієнт відповідає, цей хеш вже включений в ACK-пакет. Далі сервер перевіряє ACK і, в разі успішної перевірки, йому залишається тільки виділити пам’ять для з’єднання. Для використання цього механізму необхідно, щоб його підтримували всі сервера, які беруть участь в обміні трафіком.

Також потрібно використовувати налаштування стеку. Це налаштування використовується в якості однієї з тимчасових заходів можна налаштувати стек TCP, зменшивши тайм-аут звільнення пам’яті, виділеної для з’єднання, а також тайм-аут блокування вхідних з’єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з’єднань через затримки і нестабільних каналів.

Найефективніший спосіб захисту від SYN-flood атак, це використання міжмережного екрану, який має механізм перешкоджання поведінки SYN-атак. Принцип дії такого екрану полягаю у наступному. Коли захищаємому серверу надсилається пакет із запитом на встановлення з’єднання, міжмережний екран реєструє його в таблиці і дозволяє пакету пройти. Після приходу відповіді сервера про підтвердження запиту на з’єднання міжмережний екран посилає пакет сервера з підтвердженням з’єднання, а також посилає у відповідь пакет клієнту. З цього моменту в міжмережевому екрані активізується внутрішній таймер, що відраховує період часу, протягом якого повинен прибути пакет з підтвердженням від клієнта. Якщо запит про з’єднання нормальний, то протягом встановленого проміжку часу клієнт посилає відповідний пакет з підтвердженням з’єднання. Отримавши цей пакет, міжмережний екран буде вважати запит про встановлення з’єднання нормальним і зупинить таймер. Якщо клієнт не відповідає протягом максимально

дозволеного проміжку часу, міжмережний екран посилає спеціальний пакет серверу, що призведе до видалення інформації про з'єднання.

Застосування описаної процедури для будь-якого сервера дозволяє міжмережевому екрану запобігати заповненню черги запитів на з'єднання, оскільки всі з'єднання будуть встановлюватися відразу після того, як відповідні пакети сервера досягнутий брандмауера і будуть видалені з черги, отже, SYN атаки не зможе бути реалізована.

Захист від DDoS-атака, типу UDP-flood, більш складний. Через те, що перевірка UDP трафіку дуже складна, велика кількість операторів зв'язку пропонують своїм клієнтам блокування трафіку за різними критеріями, що є спасінням мережі за допомогою блокування окремих серверів.

Найбільш актуальним засобом боротьби з цим типом атак, є отримання всього об'єму трафіку, а далі робити детальний аналіз цього трафіку. Враховуюче те, що об'єми атака можуть бути дуже великими, доцільно буде використання хмарних технологій нарощування пропускної здатності каналів, у потрібний час.

Також для захисту від UDP-flood потрібно встановити обмеження на кількість звернень до відкритих портів, а невикористовувані порти закрити засобами апаратних або програмних міжмережевих екранів в ключових точках мережі.

HTTP-атаки дуже важко відрізнити від дійсного трафіку, оскільки вони використовують стандартні URL-запити. Це робить їх одним із найдосконаліших викликів безпеки вразливості, з якими сьогодні стикаються сервери та програми. Традиційне виявлення, засноване на швидкості, неефективне при виявленні атак HTTP-повеней, оскільки обсяг трафіку в HTTP-потоках часто перевищує порогові значення. Тому можна використати спосіб захисту – налаштування обмежень клієнтських сесій або встановлювати дорогий апаратний комплекс, який буде здійснювати аналіз та очистку трафіку.

Найефективніший механізм зменшення наслідків покладається на комбінацію методів профілювання трафіку, включаючи виявлення репутації IP-адрес, відстеження ненормальної активності. Тобто для захисту від HTTP-flood, доцільно використовувати технологію WAF, тому що завдяки цієї технології можна визначити поведінку нормального користувача, завдяки послідовної поведінки у межах нормальних параметрів, тоді як у зловмиснику все відбувається

навпаки. Технологія WAF робить «відбитки» нормальних користувачів і завдяки цьому, можна налаштувати непоганий захист від атак типу HTTP-flood.

Існують атаки, які використовують ICMP-запити, але підхід до боротьби з цими запитами дуже простий, потрібно встановити фільтрацію цих запитів, з параметрами прийому, наприклад, приймати тільки ті запити, які потрібні власнику мережі, або зробити ще легше и повністю відмовитись від прийняття та обробки пакетів типу ICMP. Також ICMP-запитів, виконується атака – пінг смерті. Рішенням цієї проблемі є введення до мережі додаткової перевірки розміру зібраного пакета при отриманні, яка підсумовує зміщення фрагментації всіх пов’язаних пакетів. Якщо загальна сума перевищить 65535, пакет вважається неправильним і відкидається. Подібна перевірка може проводитися і в міжмережних екранах.

Для того щоб уникнути атаки, яка використовує недоліки Network Time Protocol, власникам мережі потрібно слідкувати за оновленням протоколів, які вони використовують, тому що атаці підтверджені тільки користувачі версії до 4.2.7, тобто всі хто не хочуть бути атаковані завдяки цього протоколу, або самі бути учасниками таких атака, потрібно відновлювати софт. Адміністраторам завжди потрібно слідкувати за виходом нового або оновленого ПЗ, бо дуже часто недоліки минулих версій виправлені у наступних.

Отже на сьогоднішній час з’явилася велика кількість причин, що можуть визвати організування DDoS-атаки, тобто сьогодні люди можуть використовувати цей тип атак, через їх простоту реалізації, для вимагання грошей або отримання того, що вони бажають. Або це може бути проста боротьба з конкурентами, бо наслідки DdoS-атак, є цілком неприємними, починаючи з великих грошових витрат на відновлення роботи сервісу, який був атаковано, закінчуючи втратою всієї клієнтської бази через погіршення репутації, або втрати персональних даних користувачів.

В даний час великий розвиток отримала група засобів протидії, яка призначена для боротьби з потужними атаками. Але ці засоби протидії дуже дорогі та призначені для великих мереж або компаній. Засоби, що можуть використовувати невеликі підприємства не набули достатнього розвитку, через те, що у минулому такі мережі не були сильно схильні до такого типу атак.

На основі опрацювання певної інформації, я на сьогоднішній день найефективнішим засобом протидії DDoS-атака, є гібридний підхід. Цей метод

включає в себе захист за допомогою рішень зі сторонніх ресурсів і рішення захисту на стороні власника мережі. Тобто у цьому випадку ми можемо використовувати найефективніші засоби захисту мережі, які прийняли локально, а, наприклад, WAF та інші засоби фільтрації трафіку, і поєднати все це з хмаровими технологіями захисту від DDoS-атак, приклад використання захисту з хмаровими технологіями наведено на рисунку 3.6. Так, це не є економічним рішенням протидії атакам, але у разі досягнення зловмисником своєї мети, витрати можуть бути значно більшими.

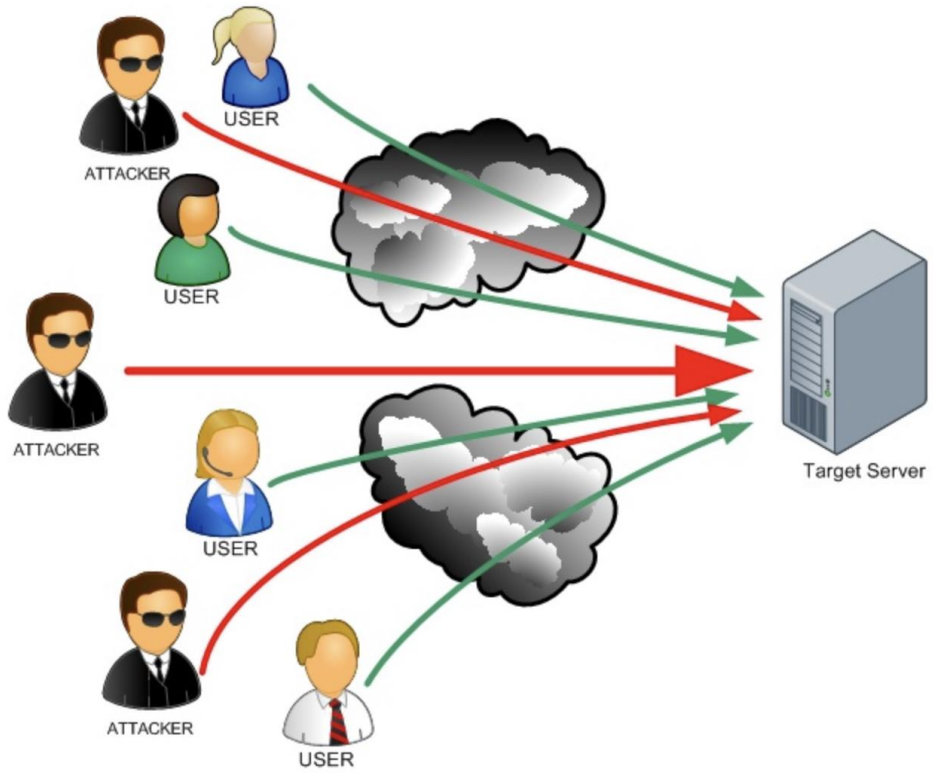

Рисунок 3.6 – Використання хмарних технологій, як захист від DDoS-атак

4 ПІДПРИЄМСТВО ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

4.1 Ситуаційний план підприємства

Підприємство, у якому циркулює інформація з обмеженим доступом, розташоване на 5-му поверсі цегляного будинку за адресою: м. Харків, вул. Волонтерська, буд. 50.

Режимна територія та приміщення цілодобово охороняються черговою зміною організації, що здійснює охорону – Товариства з обмеженою відповідальністю "Охрана и безопасность".

В радіусі 200 м знаходяться три шістнадцятиповерхові та дві двоповерхові будівлі. Вікна приміщення виходять на південний схід. На цій території розташована посадка дерев. Навпроти вікон приміщення немає будівель, з яких можливе спостереження та розвідка, але є напрямки, сектори та зони, з яких є можливість здійснення ТР з метою зняття конфіденційної інформації (план зображений схематично на рис. 4.1).

Основні характеристики вулиць, що проходять поруч з будинком, в якому розташований ОІД, наведено в табл. 4.1.

Таблиця 4.1 – Основні характеристики вулиць

№ з/п	Назва вулиці	Розташування відносно ОІД	Ширина Частини Для проїзду, м	Ширина Пішохідної Частини, м	Інтенсивність Руху автотранспорту	Наявність місць неконтрольованого перебування автотранспорту
1	Вулиця Чередниченківська	Північ	5	2,5	Середня	Так
2	Провулок Трохимівський	Північ	3	1	Низька	Так

Об'єкти, що оточують будинок, в якому розташовано ОІД наведено в табл. 4.2.

Таблиця 4.2 – Об’єкти, що оточують будинок

№	Розташування відносно ОІД	Кількість поверхів	Адреса	Характер діяльності	Відстань від ОІД, (м)
1	Північний захід	2	Вул. Чередниченківська,15	Житловий будинок	88
2	Захід	16	Вул.Волонтерська,54	Житловий будинок	86
3	Північ	2	Пров.Трохимівський,8	Житловий будинок	87
4	Північний схід	16	Вул.Волонтерська,52	Житловий будинок	98
5	Схід	16	Вул. Волонтерська, 48	Житловий будинок	97

Схему ситуаційного плану підприємства наведено на рисунку 4.1.

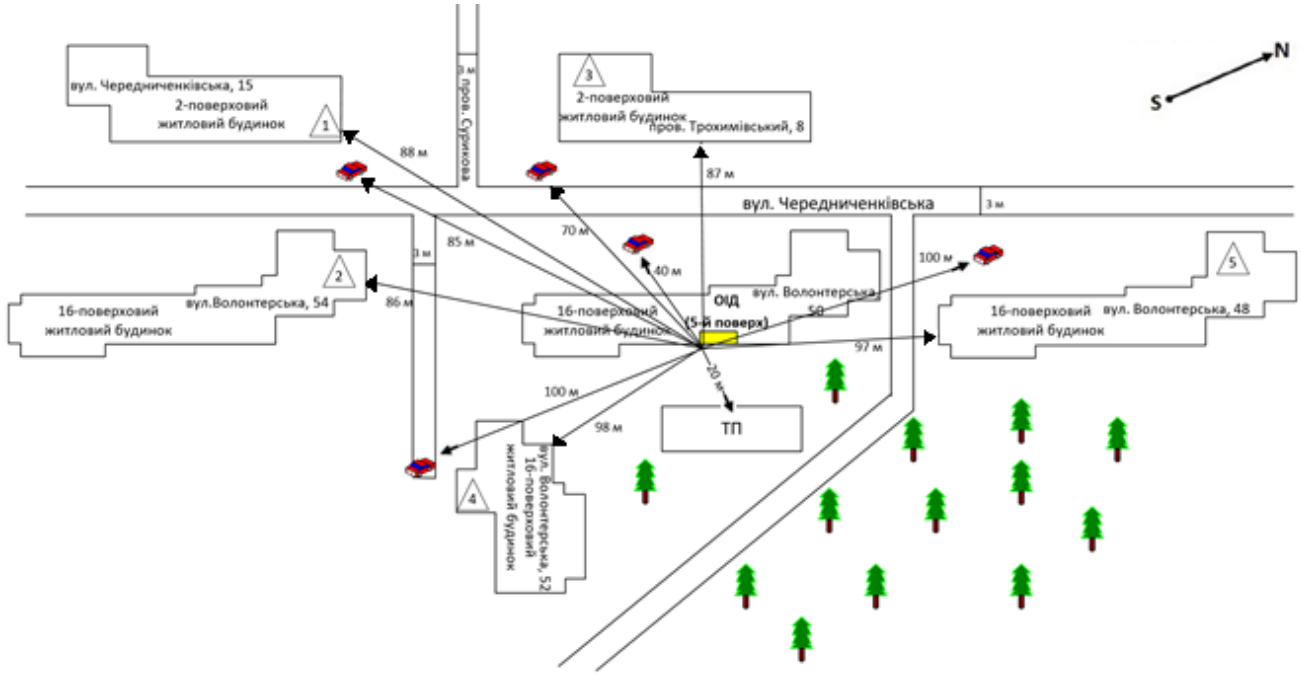

Рисунок 4.1 – Ситуаційний план підприємства

Умовні позначення:

 - місце можливого розташування та застосування рухомих ТЗР;

 - місце можливого розташування та застосування стаціонарних ТЗР;

ТП -трансформаторна підстанція.

4.2 Генеральний план підприємства

Підприємство розташоване на 5-му поверсі будинку. Стіни, підлога, стеля – капітальні. Висота над рівнем землі – 10 м.

Підприємство має одне вікно з пластиковою рамою. Вікно обладнане ролетами, виходить у бік посадки дерев в східному напрямку, розташоване на висоті 80 см від підлоги та на висоті 25 м від землі. Розмір вікна: - висота 1,80м,– ширина 2,50 м.

Параметри приміщення:

Підприємство має площу 200 квадратних метрів. Стеля звичайна залізобетонна, висота стелі 2,8 м, відстань між стелею та міжповерховим перекриттям становить 1,0 м. Підлога залізобетонна, покрита пліткою, двері броньовані металеві 1,8×0,9 м, одинарні. Двері обладнані двома механічними замками. Стіни цегляні, перекриття залізобетонні.

Освітлення підприємства: 9-ти ламповий світильники денного освітлення.

Ремонт приміщення не проводився з 2016 року.

Доступ до приміщення обмежений.

У приміщенні №5 проходить основна робота з клієнтами, та обробка конфіденційної інформації.

На рис. 4.2 наведено генеральний план підприємства.

Електроживлення приміщення здійснюється від трансформаторної підстанції ТП. Вона має сторонніх споживачів.

Схеми електроживлення, освітлення та заземлення наведені на плані, рисунок 4.2.

Систему охоронної сигналізації прокладено у кімнаті №2 та виведено усю інформацію на ПК, також на телевізорах у кімнаті охорони виведено зображення з камер спостереження.

Приміщення обладнано системою пожежної сигналізації, датчиками руху, датчиком розбиття вікон. Кінцеві лінії цієї системи виведено на пульт, який розташований в цьому будинку на першому поверсі.

Система опалення – тепла підлога, та батарея опалення.

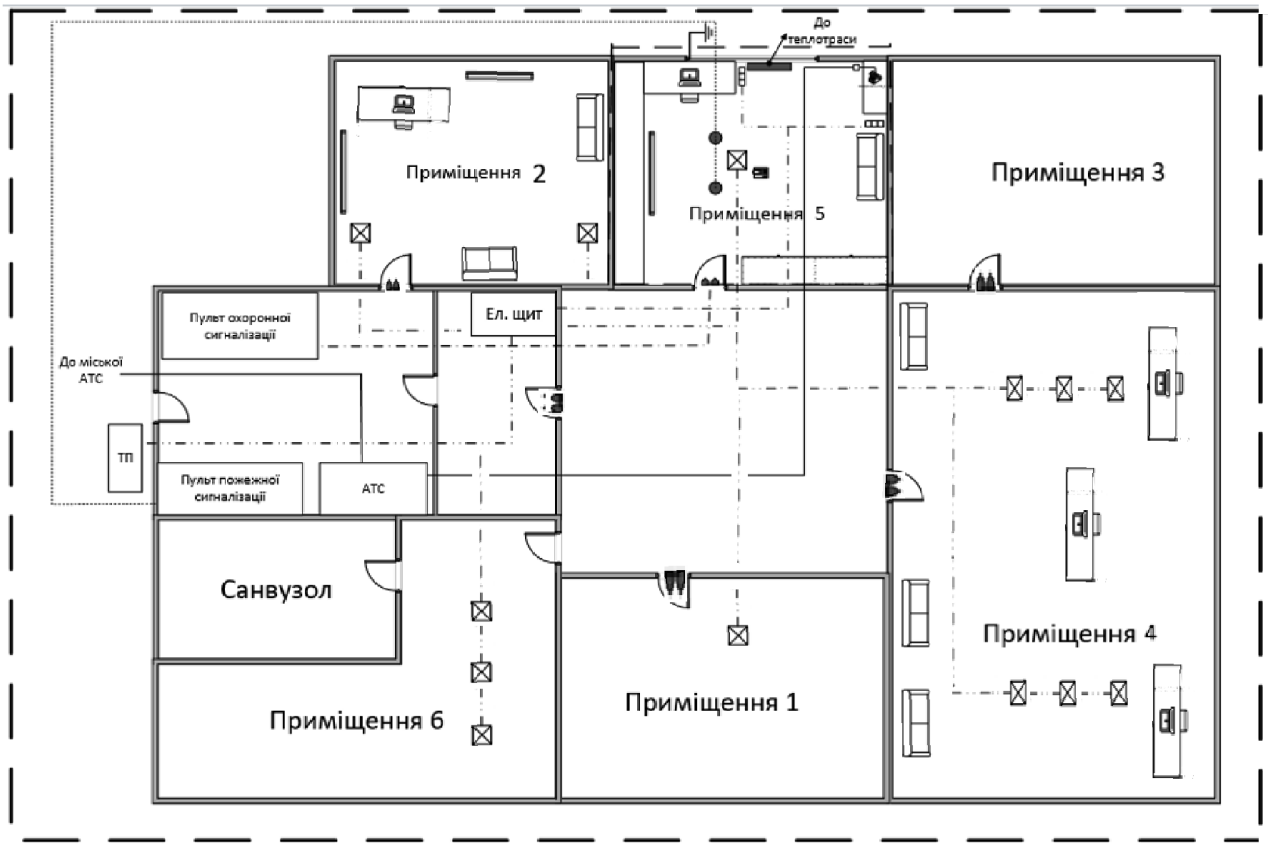

Рисунок 4.2 – Генеральний план підприємства

Умовні позначення:

- датчик на відкриття дверей
- контури об’єкту
- датчик пожежної сигналізації
- межа контрольованої зони
- батарея опалення
- кабель телефонної лінії
- ТА внутрішнього зв’язку
- кабель охоронної сигналізації
- світильник
- кабель пожежної сигналізації
- ПЕОМ
- кабель електроживлення
- ел. Розетка
- шина заземлення
- перемикач телефонної лінії
- система заземлення
- проектор
- датчик сигналізації на відкриття вікна

Перелік ОТЗ, розміщених у підприємства наведено в табл. 4.3.

Таблиця 4.3 – Основні технічні засоби

№	Найменування технічного засобу	Тип	Серійний номер
1	Системний блок у складі 5 шт	Acer	913881
	Материнська плата 5 шт	Asus PRIME B350	DFG0981
	Центральний процесор 5 шт	Intel Core i5 – 8100	91818FG
	НЖМД 5 шт	Kingston SSD 256 Гб HDD 1Тб	145DFG43
	ОЗП 5 шт	HyperX 16 ГБ	WB32G12
	Корпус 5 шт	Grey	E222GH
	Блок живлення 5 шт	CHIEFTEC 600W	81718291313
2	Клавіатура 5 шт	STEELSERIES APEX 100	GF9FD000
3	Маніпулятор «миша» 5 шт	STEELSERIES RIVAL 100	MM - 9899
4	Монітор 5 шт	Монітор 24" IPS QHD+	516H01992GKQ
5	МФУ 5 шт	Epson LaserJet	381689291
6	Телевізор SAMSUNG 3 шт	UE43AU7100UXUA	1928319313111

Опис ДТЗС. Перелік ДТЗС, які встановлено у приміщені, наведено в табл.4.4.

Таблиця 4.4 – Перелік допоміжних технічних засобів

№	Найменування, тип ТЗПІ та ДТЗС	Кількість	Призначення

1	Датчик охоронної сигналізації дверний AJAX	12	Охоронна сигналізація
2	Датчик охоронної сигналізації на відкриття вікна AJAX	1	Охоронна сигналізація
3	Датчики пожежної сигналізації AJAX	6	Пожежна сигналізація

Продовження таблиці 4.4

4	Охоронна сигналізація AJAX	1	Охоронна сигналізація
5	Датчик руху AJAX	5	Охоронна сигналізація
6	Датчик розбиття вікон AJAX	1	Охоронна сигналізація

До ОІД не заходять лінії радіофікації, оповіщення, годинофікації, та стояки системи водопостачання.

Вентиляція приміщення здійснюється природно через канали вентиляції, які проходять з горища будинку.

За межі контрольованої території виходять:

- труби водяного опалення приміщення, що підведені через суміжні приміщення та підключені до міської мережі теплопостачання;

- лінії телефонного зв’язку, що підключені до міської АТС;

- електричний кабель

- шина та заземлювач системи заземлення.

Схема підведення труб водяного опалення та схема підведення ліній телефонного зв’язку наведені на плані рисунку 4.2.

4.3 Характеристика і опис технічних каналів виток ІзОД

У приміщенні розголошується конфіденційна інформація, проводиться робота по наданню юридичних послуг громадянам, робота з документами та обробка електронно-інформаційних ресурсів. У цьому приміщенні є комп’ютери,

які обробляють конфіденційну інформацію, тому необхідно визначити канали витоку ІзОД, які існують на ОІД.

Розглянемо акустичний канал витоку ІзОД, який може бути створений:

1) шляхом безпосереднього прослуховування розмов, що ведуться на підприємстві, без застосування спеціальних засобів ТР. Найбільш сприятливі умови для прослуховування створюються під час циркуляції мовної ІзОД у приміщенні №2, №4, №5, із-за недостатньої звукоізоляції стін та дверей;

2) шляхом перехоплення мовних сигналів за допомогою портативних технічних засобів акустичної розвідки (диктофонів та магнітофонів) за межами режимного приміщення. Ці засоби можуть використовувати спеціальні вмонтовані та виносні мікрофони.

3) шляхом застосування мікрофонів направленої дії (МНД) та акустичних антен, що встановлюються в зоні прямої видимості з вікон кімнати № 5.

Враховуючи умови і особливості розташування ОІД, а також граничну допустиму відстань, з якої може використовуватися МНД (до 70 м), то вірогідність, що інформація буде знята за допомогою МНД, є великою.

Утворення віброакустичного каналу витоку ІзОД можливе завдяки вібраційним коливанням, спричиненим акустичним полем голосу, що розповсюджуються будівельними конструкціями та жорсткими інженерними комунікаціями, елементи яких виходять за межі контрольованої території внаслідок недостатньої віброізоляції шибок віконного отвору у режимному приміщенні, недостатніх віброізоляційних властивостей труб систем водяного опалення.

Приймання таких коливань може здійснюватися шляхом:

1) застосування портативних засобів акустичної розвідки із записом інформативних сигналів на магнітні носії;

2) дистанційного встановлення з відстані до 25м високочутливих вібродатчиків.

Враховуючи такі умови приміщення підприємства, як труби центрального опалення та шибки віконного отвору, віброізоляція яких не є достатньою, імовірність застосування вібродатчиків є достатньо високою.

Лазерний акустичний канал витоку ІзОД утворюється за рахунок дистанційного перехоплення вібраційних коливань жорстких поверхонь, що

виникають під впливом акустичного поля мови, лазерними засобами акустичної розвідки, які встановлюються в зоні прямої видимості з вікон кімнати № 5.

Враховуючи умови і особливості розташування приміщення № 5, імовірність застосування ЛЗАР є високою, тому що навколо будівлі, в якій розміщений ОІД, в межі 100 метрів розміщенні будівлі, з яких можливо зняти інформацію за допомогою ЛЗАР, а гранична допустима відстань для використання ЛЗАР в міських умовах складає близько 200 м.

Акустоелектричний канал може бути створений шляхом:

– поширення інформативних акустичних сигналів дротовими лініями технічних засобів, які мають «мікрофонний ефект», наприклад, лінії відкритого телефонного зв’язку та їх приймання засобами ТР, які підключаються до дротових ліній, що виходять за межі контрольованої території;

– електромагнітного ВЧ-випромінення, модульованого інформативним мовним сигналом. Джерелами цих акустоелектричних перетворень можуть бути електронні схеми ДТЗС.

Перехоплення засобами ТР інформативних сигналів ведеться із застосуванням радіоприймальних пристроїв систем і комплексів радіоелектронної розвідки в діапазоні частот від одиниць Гц до одиниць ГГц. В залежності від потужності електромагнітних випромінювань дальність ведення ТР може складати від десятків до сотень метрів.

Імовірними місцями розміщення та застосування засобів ТР є:

– місця прокладення дротових ліній міського зв’язку, що виходять за межі контрольованої території;

– місця розташування стаціонарних та тимчасових ЗТР, які показані на ситуаційному плані рисунку 4.1;

– трансформаторна підстанція (ТР), яка знаходиться у 20 м у східному напрямі;

– кімнати на поверх вище та на поверх нижче, та вузол електроживлення всього будинку, в якому знаходиться ОІД.

Канали витоку ІзОД за рахунок ПЕМВН утворюються:

– електричними та магнітними полями, які виникають під час роботи ОТЗ і ДТЗС;

– внаслідок взаємного впливу між ланцюгами, якими передається ІзОД;

– внаслідок стікання струмів інформативного сигналу в ланцюги заземлення;

– внаслідок «паразитної» генерації, що виникає в блоках ОТЗ і ДТЗС;

– внаслідок впливу електричних, магнітних або акустичних полів небезпечного сигналу на ДТЗС.

Перехоплення ПЕМВН здійснюється шляхом приймання та аналізу електромагнітних випромінювань, які виникають під час роботи встановлених у кімнаті №2, №4, №5 ОТЗ і ДТЗС, а також наводив інформативних сигналів в лініях зв'язку, які виходять за межі КЗ.

Канали витоку ІзОД за рахунок побічних електромагнітних випромінювань і наводок (ПЕМВН) утворюються:

– електричними та магнітними полями, які виникають під час роботи ОТЗ і ДТЗС;

– внаслідок взаємного впливу між ланцюгами, якими передається ІзОД;

– внаслідок стікання струмів інформативного сигналу в ланцюги заземлення;

– внаслідок «паразитної» генерації, що виникає в блоках ОТЗ і ДТЗС;

– внаслідок впливу електричних, магнітних або акустичних полів небезпечного сигналу на ДТЗС.

Розповсюдження ПЕМВН на значні відстані обумовлює можливість застосування для ТР спеціальних стаціонарних або портативних радіоприймальних пристроїв в діапазоні частот від одиниць Гц до 1 ГГц, які здатні вести розвідку на відстані близько 100 м.

Імовірними місцями розміщення та застосування засобів ТР є:

– місця прокладення дротових ліній міського зв'язку, що виходять за межі контрольованої території;

– приміщення будинку, що знаходиться на відстані 86 м у західному напрямі по вулиці Волонтерській (буд. №54);

– приміщення будинку, що знаходиться на відстані 88 м у південно-західному напрямку на вулиці Чередниченківській (буд. №15);

– приміщення будинку, що знаходиться на відстані 87 м у північно-західному напрямку по провулку Трохимівському (буд. №8);

– приміщення будинку, що знаходиться на відстані 98 м у південному напрямку по вулиці Волонтерській(буд. №54);

– приміщення будинку, що знаходиться на відстані 97 м у північно-східному напрямку по вулиці Волонтерській(буд. №48).

Канал ВЧ-нав’язування – канал витоку ІзОД, що утворюється шляхом передавання високочастотних коливань в лінію відкритого міського телефонного зв’язку, що виходить за межі контрольованої території.

Найбільш імовірними місцями розміщення і застосування засобів ТР є місця прокладення дротових ліній міського зв’язку, що виходять за межі контрольованої території.

Таблиця 4.5 – Перелік можливих загроз ОІД у приміщенні підприємства

Канал витоку інформації	Пристрої для зняття інформації	Джерело інформації	Вид інформації, що може бути знята
Акустичний канал	Закладні пристрої, направлені мікрофони	Розмова людини, звуковідтворююча апаратура	Конфеденційна інформація
Віброакустичний канал	Стетоскопи	Розмова людини, звуковідтворююча апаратура	Конфіденційна інформація
Лазерний акустичний канал	Використання методу ЛЗАР для зняття інформації зі скляних поверхонь	Розмова людини, звуковідтворююча апаратура	Конфіденційна інформація
Акустоелектричний канал	Зняття інформації за допомогою підключення до сполучних ліній ДТЗС	Розмова людини, звуковідтворююча апаратура	Конфіденційна інформація
Канали ПЕМВН	Зняття інформації від ОТЗ та ДТЗС каналами перехоплення ПЕМВ приймачем та перетворення сигналу технічними засобами	Основні та допоміжні технічні засоби та системи	Конфіденційна інформація
Канал ВЧ-нав’язування	Зняття інформації шляхом контактного введення струмів високої частоти від відповідного генератора в лінії.	Розмова людини та звуковідтворююча апаратура	Конфіденційна інформація

Візуально-оптичний канал	Оптичні засоби розвідки	Екран комп'ютера, мультимедійна та звичайна дошки	Конфіденційна інформація

Перелік можливих загроз для ОІД, який знаходиться на підприємстві, представлений у табл. 4.5.

Візуально – оптичний канал витоку ІзОД утворюється за рахунок отримання технічними засобами розвідки, що встановлюються в зоні прямої видимості з вікна ОІД, видової інформації у вигляді зображень документальної ІзОД в паперовому вигляді, а також обстановки на ОІД.

Отримання вказаної інформації може здійснюватися шляхом дистанційної зйомки та спостереження з використанням залежно від умов спостереження (відстані до ОІД, освітленості тощо) засобів оптико – електронної та візуально – оптичної ТР.

Враховуючи умови і особливості розташування приміщення підприємства, оснащеність вікон ОІД ролетами, можливість ефективного застосування вказаних засобів ТР є малоймовірною.

5 ВИБІР СТРУКТУРИ КСЗІ ПІДПРИЄМСТВА

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності [21].

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також [21]:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити [21].

Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережних екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

У процес створення КСЗІ залучаються такі сторони [21]:

- організація, для якої здійснюється побудова КСЗІ;

- організація, що здійснює заходи з побудови КСЗІ;

- Адміністрація Державної служби спеціального зв'язку та захисту інформації України;

- організація, що здійснює державну експертизу КСЗІ;

- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ.

Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації. Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх змінних параметрах. Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, заземлення та інші [21].

Залежно від виду та форми подання інформаційних сигналів, які циркулюють в інформаційно-телекомунікаційній системі, у тому числі і в автоматизованих системах, при побудові КСЗІ можуть використовуватися різні засоби захисту.

Перш ніж пропонувати будь-які рішення щодо організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки – набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта структури цінностей і проведення аналізу ризику, і визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис загальної мети побудови системи безпеки об'єкта, що виражається через сукупність факторів або критеріїв, які уточнюють мету. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні [21].

Розробка політики безпеки організації, як формальної, так і неформальної, – безумовно, нетривіальне завдання. Експерт повинен не тільки знати відповідні стандарти і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але й, наприклад, проявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів з організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей: необхідно за деяким критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити такі процеси, пов'язані з розробкою і реалізацією політики безпеки.

1) Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2) Заходи з оцінювання відповідності заходів щодо забезпечення захисту інформації системи деякого еталонного зразка: стандарт, профіль захисту тощо.

3) Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданої з безпеки.

4) Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій безпеки для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом, створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно. Відзначимо лише, що для розробки моделей застосовується широкий спектр математичних методів (моделювання, теорії інформації, графів і ін.).

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі. Слід відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом, тільки дають можливості надійного управління доступом або інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі:

– всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Множина об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу [22].

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій щодо розмежування доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне управління доступом, що має на увазі:

– всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність, яка міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакові значення, кажуть, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру, і, таким чином, в системі можна реалізувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вища його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт, крім рівня прозорості має поточне значення рівня безпеки, яке може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів в верхні. При цьому вона функціонує на тлі виборчої політики, надаючи їй вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Вибір політики безпеки – це прерогатива керівника системи захисту інформації. Але якою б вона не була, важливо, щоб впроваджена система захисту інформації відповідала вимогам.

Перелік основних завдань, які повинні вирішуватися комплексною системою захисту інформації, наведено на рис. 5.1 [22]:

Рисунок 5.1 – Завдання КСЗІ

– управління доступом користувачів до ресурсів АС з метою її захисту від неправомірного випадкового або навмисного втручання в роботу системи та несанкціонованого (з перевищенням наданих повноважень) доступу до її інформаційних, програмних і апаратних ресурсів з боку сторонніх осіб, а також осіб з числа персоналу організації та користувачів;

– захист даних, що передаються по каналах зв'язку;

– реєстрація, збір, зберігання, обробка і видача відомостей про всі події, що відбуваються в системі і які стосуються її безпеки;

– контроль роботи користувачів системи з боку адміністрації та оперативне сповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль і підтримку цілісності критичних ресурсів системи захисту та середовища виконання прикладних програм;

– забезпечення замкнутого середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему

потенційно небезпечних програм і засобів подолання системи захисту, а також від впровадження і розповсюдження комп'ютерних вірусів;

– управління засобами системи захисту.

5.1 Структура КСЗІ та вимоги до її елементів

Комплексна система захисту інформації в приміщенні складається з підсистем, що наведено на рис. 5.2.

Рисунок 5.2 – Підсистеми комплексної системи захисту інформації

Підсистема захисту інформації від витоку технічними каналами призначена для блокування витоку інформації за рахунок побічних випромінювань і наведень, повинна бути реалізована засобами активного радіотехнічного маскування – генератором просторового зашумлення типу «РІАС-1М». Живлення генератора шуму здійснити від того ж джерела, що й живлення ТЗ ЕОТ.

Підсистема захисту ІзОД від несанкціонованого доступу призначена для блокування несанкціонованих дій користувачів (зловмисників), повинна бути реалізована програмними засобами комплексу засобів захисту «Лоза-1» та організаційними заходами.

Підсистема захисту від шкідливого ПЗ призначена для захисту від вірусів, їх виявлення та вилучення (лікування), повинна бути реалізована програмою ESET.

Для захисту від шкідливого програмного забезпечення повинні бути вжиті заходи, що наведені на рис. 5.3.

Рисунок 5.3 – Заходи захисту від шкідливого ПЗ

Файли для оновлення адміністратор безпеки інформації отримує від фірми-постачальника антивірусного програмного забезпечення.

Захист від витоку ІзОД за рахунок наведень на лінії електроживлення здійснюється установкою на лінії електроживлення ІС фільтру захисного протизавадного типу «М - 17». Для гальванічної розв’язки кіл живлення основних та допоміжних технічних засобів від електричної мережі та захисту інформації, що обробляється в технічних засобах від витоку колами живлення змінного струму, електроживлення основних та допоміжних засобів обробки інформації здійснити через розділовий трансформатор «РІАС-4ТР/15».

Система захисного заземлення – автономний контур заземлення технічних засобів ІС повинен бути виконаний в межах контрольованої зони.

Захист від витоку ІзОД за рахунок наведень на лінію телефонного зв’язку здійснювати шляхом відключення цієї лінії у місці її входу у приміщення за допомогою перемикача під час обробки ІзОД на ІС.

Захист від атак відмова в обслуговуванні потрібно здійснювати найефективнішим засобом протидії, а саме гібридний засіб захисту. Цей метод

включає в себе захист за допомогою рішень зі сторонніх ресурсів і рішення захисту на стороні власника мережі. Тобто у цьому випадку ми можемо використовувати найефективніші засоби захисту мережі, які прийняли локально, а, наприклад, WAF та інші засоби фільтрації трафіку, і поєднати все це з хмаровими технологіями захисту від DDoS-атак. Так, це не є економічним рішенням протидії атакам, але у разі досягнення зловмисником своєї мети, витрати можуть бути значно більшими.

Гібридний підхід, який використовує відбір трафіку на рівні провайдеру для уникнення лавиноподібних атак і рішення для захисту системи, які використовує власник серверу, вважається оптимальним при захисті від DDoS-атак.

Послуги щодо захисту від DDoS надаються операторами зв'язку, провайдерами або іншими захисними компаніями. Вони роблять моніторинг трафіку в реальному часі, для того щоб знайти або засікти аномальний трафік. Також займаються захисними функціями, які дозволяють приховати обладнання клієнта від зловмисників, заборонивши до нього доступ з інтернету, застосовують інтелектуальні системи.

Тобто гібридні захисти вдають із себе комплекс захисних актів, які складаються з локальних методів захисту та допомоги ззовні. Це можуть бути як хмарні технології, так і надання захисту зі сторонніх ресурсів.

5.2 Умови використання засобів захисту

Умови використання засобів захисту зі складу КСЗІ ІС – звичайні.

Апаратура використовується в умовах виділеного підприємства, в якому вологість повітря, температура та атмосферний тиск відповідають вимогам розробника на кожен з типів апаратури.

Використання ПЕОМ зі складу ІС дозволяється лише за умови справних засобів захисту (контроль функціонування та працездатності засобів захисту – за інструкціями по їх експлуатації) та при відключеної лінії телефонного зв'язку.

Суттєвою умовою використання ПК для обробки ІзОД є заборона обміну мовною інформацією під час обробки ІзОД.

Постійний догляд за співробітниками підприємства та моніторинг трафіку, який поступає до локальної мережі підприємства. Використання високошвидкісного інтернету завдяки оптичного волокна.

Перевірка робочих місць перед початком робочого дня, використання електронних турнікетів, які надають інформацію по кожному робітнику нашого підприємства: час коли заходив та виходив, особиста інформація людини.

Налаштування прав доступу до інформації для кожного співробітника, слідкування за аудитом системи та журналом дії кожного робітника.

Контролювання потоку клієнтів, запобігання черг на підприємстві, використання електронної черги та завчасної записи.

5.3 Управління КСЗІ та взаємодія її елементів

Управління КСЗІ здійснюється безпосередньо з АРМ (персонального комп'ютера).

Засоби активного захисту від витоку ІзОД каналами ПЕМВН повинні бути розташовані безпосередньо на робочих місцях робітників, за умови забезпечення доступу до органів управління й контролю.

Управління засобами захисту полягає в тому, що засоби захисту від витоку каналами ПЕМВН та наведень на мережу електроживлення вмикаються в роботу при подачі живлення на апаратуру ІС, а управління доступом до ресурсів ПЕОМ здійснюється за допомогою комплексу засобів захисту «Лоза-1» та засобів адміністрування ОС ПЕОМ.

Під час обробки ІзОД на ІС лінія телефонного зв’язку має бути відключеною за допомогою перемикача.

Засоби захисту EIP контролюються віддалено, завдяки послуг сторонніх ресурсів, а саме хмарні технології, у цьому випадку ми маємо постійно актуальну копію системи на хмарному носії. Контролюється кількість трафіку, який отримає наша система, та проводиться його на моніторинг на сторонні або зловмисні пакети, для запобігання перенавантаження системи, для уникнення лавиноподібних атак. Також для захисту електронної інформації будемо використовувати WAF, керувати цим фаєрволом та налаштовувати його стосовно нашого підприємства, буде окрема людина, яка також працюватиме віддалено, для постійного контролю системи у разі спроби атаки зловмисниками.

Ми маємо можливість обмежити розмір пам’яті сервера для кожного вхідного пакета. Також потрібно використовувати cookie, тобто використовувати криптографічне хешування.

Також потрібно використовувати налаштування стеку. Це налаштування використовується в якості однієї з тимчасових заходів можна налаштувати стек TCP, зменшивши тайм-аут звільнення пам’яті, виділеної для з’єднання, а також тайм-аут блокування вхідних з’єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з’єднань через затримки і нестабільних каналів.

Ми будемо використовувати міжмережний екран. Коли захищаємому серверу надсилається пакет із запитом на встановлення з’єднання, міжмережний екран реєструє його в таблиці і дозволяє пакету пройти. Після приходу відповіді сервера про підтвердження запиту на з’єднання міжмережний екран посилає пакет сервера з підтвердженням з’єднання, а також посилає у відповідь пакет клієнту. З цього моменту в міжмережному екрані активізується внутрішній таймер, що відраховує період часу, протягом якого повинен прибути пакет з підтвердженням від клієнта. Якщо запит про з’єднання нормальний, то протягом встановленого проміжку часу клієнт посилає відповідний пакет з підтвердженням з’єднання. Отримавши цей пакет, міжмережний екран буде вважати запит про встановлення з’єднання нормальним і зупинить таймер. Якщо клієнт не відповідає протягом максимально дозволеного проміжку часу, міжмережний екран посилає спеціальний пакет серверу, що призведе до видалення інформації про з’єднання.

5.4 Схемні рішення стосовно розміщення основних технічних засобів ЕОТ, технічних засобів захисту, мережі живлення та заземлення

На рис. 5.1 наведено схему розміщення основних технічних засобів захисту приміщення.

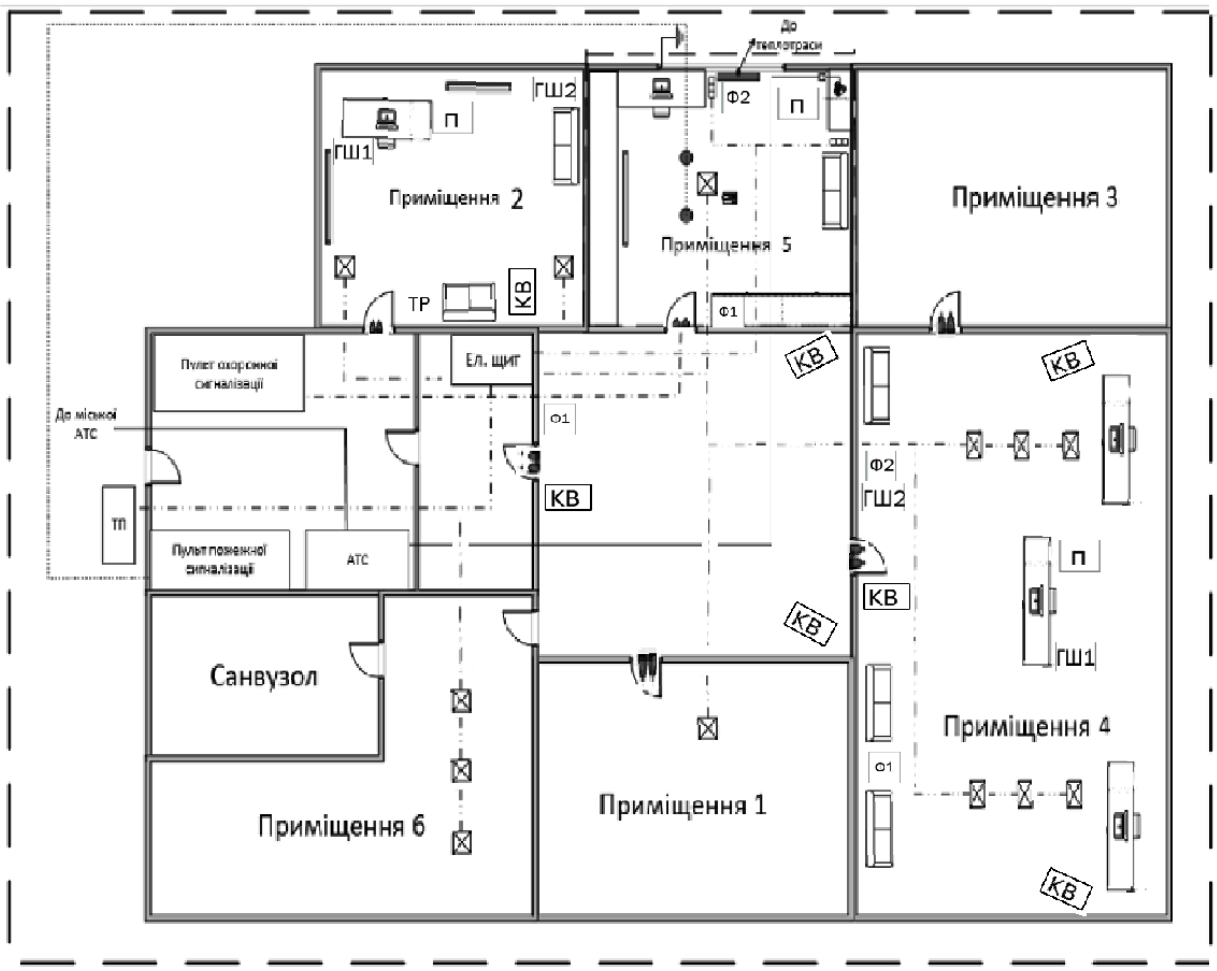

Рисунок 5.2 – Схема розміщення основних технічних засобів захисту приміщення

Умовні позначення:

Ф1 - Мережний фільтр «М-17»;

Ф2 - Мережний фільтр «М-9»;

ТР - Розділовий трансформатор «PIAC-4TP/15»;

П - Переимикач на телефонну лінію;

ГШ1 - Генератор шумових сигналів;

ГШ2 - Генератором високочастотного шуму «PIAC-1M».

КВ – камера відеоспостереження.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було реалізовано завдання на роботу та досягнуто її мети – запропоновано комплексну систему захисту електронних інформаційних ресурсів на технічному рівно та мережному.

В кваліфікаційній роботі проаналізовано поняття електронних інформаційних ресурсів, розглянуто можливі засоби захисту від атак типу відмови в обслуговуванні та засоби захисту можливих каналів витоку інформації.

Підприємство володіє не найкращім місцем розташування, так як оточене приміщеннями сторонніх кімнат, а вікно виходить у двір неконтрольованої території, де, поблизу, розташовуються житлові будинки, а так само місця паркування автомобілів, з яких не становить великих труднощів зняти конфіденційну інформацію, що циркулює у приміщенні.

В ході обстежень були проведені такі заходи:

– проведений аналіз розташування ОІД на місцевості для визначення можливих джерел загроз;

– досліджені інженерні комунікації, які мають вихід за межі контрольованої території;

– виявлені трасування проводів та кабелів електроживлення, заземлення, пожежної та охоронної сигналізації, а також інженерних комунікацій;

– виявлена наявність транзитних, незадіяних кабелів, кіл і проводів;

– визначені технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

– визначені технічні засоби, що потребують переобладнання та встановлення засобів ТЗІ;

– визначено модель захисту мережі підприємства від DDoS-атак.

За результатами обстеження було складено:

– ситуаційний план приміщення та його опис;

– генеральний план та його опис;

– схему розташування та опис основних технічних засобів та допоміжних технічних засобів.

На підставі проведеного аналізу загроз і вразливостей, якими є канали витоку інформації, підбору засобів захисту для кожного каналу, була розроблена і

впроваджена комплексна система захисту інформації відносно виділеного приміщення.

Результати роботи можуть бути використані як приклад комплексної системи захисту інформації на підприємстві.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Що таке DDoS-атака [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://github.com/Ha3MrX/DDos-Attack., дата звернення 01.12.2022.

2. DoS і DDoS-атаки [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://www.iseo.ru/seo-wiki/dos-ataka/, дата звернення 01.12.2022.

3. DDoS атаки в 2019 г: статистика [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://networkguru.ru/statistika-ddos-atak-2019-god/, дата звернення 01.12.2022.

4. DDoS-атаки: типи атак і рівні моделі OSI [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://firstvds.ru/technology/types-of-ddos, дата звернення 01.12.2022.

5. Захист сервера від DDoS-атак [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: https://itelon.ru/blog/zashchita-servera-ot-ddos-atak/, дата звернення 01.12.2022.

6. HTTP [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/HTTP, дата звернення 01.12.2022.

7. Інформаційні ресурси організації [Електронний ресурс]. – 2008. – Режим доступу до ресурсу: https://pidru4niki.com/10020805/informatika/informatsiyni_resursi_organizatsiyi, дата звернення 01.12.2022.

8. Що таке DDoS атака. Налаштування ефективного захисту від DDoS атак на сервер [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://rigweb.ru/support/khosting-i-domeny/tipy-ddos-atak-i-sposoby-zashchity-ot-nikh/, дата звернення 01.12.2022.

9. Що таке WAF, або захищаємо сайти і додатки від DDoS-атак [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://channel4it.com/publications/CHto-takoe-WAF-ili-zashchishchaem-sayty-i-prilozheniya-ot-DDoS-atak-33271.html.=, дата звернення 01.12.2022.

10. Що таке DDoS (Distributed Denial of Service). Як захиститися від DDoS-атак. [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://stormwall.pro/knowledge-base/termin/ddos-protection, дата звернення 01.12.2022.

11. Фільтрація трафіка [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://iptcp.net/filtratsiya-trafika.html, дата звернення 01.12.2022.

12. Запобігання атак з розподіленим відмовою в обслуговуванні (DDoS) [Електронний ресурс]. – 2008. – Режим доступу до ресурсу: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aec d8011e927_.html, дата звернення 01.12.2022.

13. DDoS-атаки: що це, походження, види і способи захисту [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://selectel.ru/blog/ddos-attacks/, дата звернення 01.12.2022.

14. DDoS-атака та брандмауер веб-додатків [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.indapoint.com/blog/ddos-attack-and-web-application-firewall.html, дата звернення 01.12.2022.

15. Чому WAF і DDoS - ідеальний заздалегідь укладений шлюб [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://blog.radware.com/security/2016/04/waf-ddos-perfect-marriage/, дата звернення 01.12.2022.

16. Безпека домашньої мережі: як забезпечити захист роутера від атак [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://eset.ua/ru/news/view/655/bezopasnost-domashney-seti-kak-obespechit-zashchitu-routera-ot-atak, дата звернення 01.12.2022.

17. DDoS-атаки [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.anti-malware.ru/threats/ddos-attack, дата звернення 01.12.2022.

18. ДОКУМЕНТАЦІЯ НОРМАТИВНА [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://www.pharmencyclopedia.com.ua/article/2575/dokumentaciya-normativna, дата звернення 01.12.2022.

19. DDoS. Відмова від обслуговування [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Distributed_Denial-of-service,_DDoS_, дата звернення 01.12.2022.

20. Протокол управління передачею (TCP) [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp, дата звернення 01.12.2022.

21. AlterSign. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс] / AlterSign // AlterSign. – 2012. – Режим доступу до ресурсу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi, дата звернення 01.12.2022.

22. Комплексні системи захисту інформації [Електронний ресурс] / Ю. Є.Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – 2018. – Режим доступу до ресурсу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil1.html, дата звернення 01.12.2022.

23. Білоус В. С. ФОРМУВАННЯ ЕЛЕКТРОННИХ РЕСУРСІВ [Електронний ресурс] / В. С. Білоус. – 2015. – Режим доступу до ресурсу: https://library.vspu.edu.ua/polki/vistupi/belous_2015_1.pdf, дата звернення 01.12.2022.

24. Поняття технічної документації. Види технічної документації. [Електронний ресурс] // Національний університет Львівського політеха. – 2019. – Режим доступу до ресурсу: https://studfile.net/preview/9821829/page:4/, дата звернення 01.12.2022.

25. База даних [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/База_даних, дата звернення 01.12.2022.

26. Юрченко О. М. Концептуальні основи захисту економічної інформації як об’єкта інтелектуальної власності. К., 2006.

27. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации: В 2 т. К., 2008;

28. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. К., 2009.

29. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних. К., 2009.

30. Конспект лекцій з дисципліни «Захист інформаційних ресурсів обмеженого доступу» для студентів спеціальності 123 «Кібербезпека» за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки» / Упоряд.: І.О. Милютченко. – Харків: ХНУРЕ, 2017. – 245 с.

31. Інформаційні ресурси: аналіз категорії та класифікація / І.О. Милютченко, Б.В. Онопко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2018. Вип. 192. С. 157– 161.