Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеня магістра

**Здобувача вищої освіти** *Полонського Геннадія Борисовича*

**академічної групи** *281м-23-2 ІДУ*

**спеціальності** *281 Публічне управління та адміністрування*

**за освітньо-професійною програмою** *281 Цифрове врядування*

**на тему:** *«Цифрові механізми забезпечення інформаційної безпеки в органах публічного управління»*

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | Квітка С. А. | | | |
| розділів: | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент:** | Мазур О. .Г | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер:** | | | | |

**Дніпро**
**2024**

# РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи магістра на тему «Цифрові механізми забезпечення інформаційної безпеки в органах публічного управління».

70 стор., 65 джерел, 9 рис.

ЦИФРОВІЗАЦІЯ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КІБЕРБЕЗПЕКА, КІБЕРЗЛОЧИННІСТЬ, ПУБЛІЧНЕ УПРАВЛІННЯ, ІНФОРМАЦІЙНІ РЕСУРСИ.

Об’єкт дослідження – процеси цифрової трансформації публічного управління.

Предмет дослідження – механізми забезпечення інформаційної безпеки в органах публічного управління в умовах цифровізації.

Мета дослідження – дослідження механізмів забезпечення безпеки інформаційних ресурсів органів публічного управління в умовах цифровізаціїх та розробка пропозицій щодо підвищення кібербезпеки в органах публічної влади.

У першому розділі досліджуються питання кібернетичної безпеки в публічному управлінні. У другому розділі висвітлено світовий досвід забезпечення кібернетичної безпеки. Третій розділ присвячено розвитку та удосконаленню механізмів забезпечення безпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування в умовах цифровізаці.

Сфера практичного застосування результатів роботи – полягає у можливості їх використання в органах публічного управління та місцевого самоврядування для забезпечення кібербезпеки інформаційних ресурсів, виконанні завдань та при проведенні навчань у віддаленому доступі для різних органів у цій сфері.

# ABSTRACT

Explanatory note of the master's qualification work on the topic «Digital mechanisms for ensuring information security in public administration bodies Mechanisms for ensuring cybersecurity in public administration bodies».

70 pages, 65 sources, 9 pictures.

DIGITALIZATION, INFORMATION SECURITY, CYBERSECURITY, CYBERCRIME, PUBLIC ADMINISTRATION, INFORMATION RESOURCES.

The object of research is the processes of digital transformation of public administration.

The subject of the study is the mechanisms for ensuring information security in public administration bodies in the context of digitalization.

The purpose of the study is to study the mechanisms for ensuring the security of information resources of public administration bodies in the context of digitalization and to develop proposals for improving cybersecurity in public authorities.

The first section examines the issues of cyber security in public administration. The second section highlights the world experience in ensuring cyber security. The third section is devoted to the development and improvement of mechanisms for ensuring the security of information resources of public administration bodies and local self-government bodies in the context of digitalization.

The scope of practical application of the results of the work is the possibility of their use in public administration and local self-government bodies to ensure the cybersecurity of information resources, perform tasks and conduct remote training for various bodies in this area.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NCSD (National Cyber Security Division) – є підрозділом Управління кібербезпеки та комунікацій Агентства з кібербезпеки та безпеки інфраструктури Міністерства внутрішньої безпеки США.

DOS (Denial of Service) – хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів (серверів), що надаються. , або цей доступ буде утруднений.

NIST (National Institute of Standards and Technology at the U.S. Department of Commerce) - NIST Cybersecurity Framework допомагає компаніям будь-якого розміру краще розуміти ризики кібербезпеки, керувати ними та зменшувати їх, а також захищати свої мережі та дані.

ЄС (Європе́йський Сою́з) – економічний і політичний союз, що об'єднує 27 незалежних держав-членів, що розташовані в Європі.

США (Сполучені Штати Америки) – федеративна президентська республіка , яка адміністративно складається з 50 штатів і федерального округу Колумбія.

DDoS (istributed denial-of-service) – атака, яка відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою.

NGFW (Next-generation firewall) – це вбудована платформа мережевої безпеки, що поєднує традиційний брандмауер з іншими функціями фільтрації мережевих пристроїв.

US-CERT (United States Computer Emergency Readiness Team) – підрозділ Національного управління кібербезпеки Міністерства внутрішньої безпеки США

CERT-EU (Computer Emergency Response Team for the European Union) – кладається з команди експертів з IT-безпеки з установ та органів ЄС.

CERT-UA (Computer Emergency Response Team of Ukraine) – спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Заснований у 2007 році.

ICO/IEC (International Organization for Standardization/ International Electrotechnical Commission) – підрозділ Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії, яке займається всіма питаннями пов'язаними зі стандартами в галузі інформаційних технологій.

EDR (Endpoint detection and response) – це інтегроване рішення безпеки кінцевої точки, яке поєднує безперервний моніторинг у реальному часі та збір даних кінцевої точки з функціями автоматизованого реагування та аналізу на основі правил.

Intune MAM (Mobile Application Management) – відноситься до набору функцій керування Intune, які дозволяють публікувати, надсилати, налаштовувати, захищати, контролювати та оновлювати мобільні програми для ваших користувачів.

Intune MDM (Mobile Device Management) – ці рішення MDM беруть на себе контроль над усім пристроєм. У результаті співробітники більше не використовуватимуть свій приватний пристрій для доступу до даних компанії, оскільки вони не хочуть, щоб їхня компанія контролювала пристрій, який їм належить.

BYOD (Bring your own device) – це IT-політика, згідно з якою співробітникам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до корпоративних даних та систем.

# ВСТУП

**Актуальність теми.** Стрімкий розвиток інформаційних технологій змінив як нормативно-правову базу, так і принципи забезпечення кібербезпеки інформаційних ресурсів органів державного управління та місцевого самоврядування. Провідними світовими державами здійснюється формування глобальних інформаційних мереж на основі наявних і новітніх систем зв'язку. Високий рівень інформаційного забезпечення інформаційних ресурсів у сучасних умовах стає визначальним фактором досягнення оперативної й технічної переваги над різного роду загрозами. Основою системи забезпечення кібернетичної безпеки є мережа, створена на базі наявних і перспективних мереж зв'язку і передачі даних із застосуванням сучасних технологій [1].

Варто констатувати, що сучасний стан забезпечення кібербезпеки інформаційних ресурсів не забезпечує у повному обсязі нейтралізацію наявних загроз і викликів. Органи публічного управління та місцевого самоврядування забезпечуються проведенням єдиної державної політики у всіх сферах життєдіяльності, системою заходів економічного, політичного та організаційного характеру, адекватним загрозам і небезпекам життєво важливих інтересів, суспільства і держави. Враховуючи той факт, що забезпечення кібербезпеки інформаційних ресурсів є багатокомпонентним, звичайно постає потреба в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цих ресурсів, тобто у забезпеченні життєздатності її системоутворюючих елементів, зокрема органів публічного управління та місцевого самоврядування. Такою метою і є забезпечення кібербезпеки інформаційних ресурсів, а також реалізації цих дій у даних органах.

Для підвищення ефективності забезпечення кібербезпеки інформаційних ресурсів даних органів управління є реалізація нових перспектив та пропозицій, яка повинна мати програмні засоби, нормативно-правову базу та використовувати міжнародний та європейський досвід для прискорення

вирішення кібернетичних атак. Таким чином, актуальність теми роботи є очевидною.

**Об'єкт дослідження –** процеси цифрової трансформації публічного управління.

**Предмет дослідження –** механізми забезпечення інформаційної безпеки в органах публічного управління в умовах цифровізації.

**Мета дослідження –** дослідження механізмів забезпечення безпеки інформаційних ресурсів органів публічного управління в умовах цифровізаціїх та розробка пропозицій щодо підвищення кібербезпеки в органах публічної влади.

Для досягнення поставленої мети роботи визначені наступні **завдання**:

– дослідити сутність цифрової трансформації публічного управління;

– обґрунтувати необхідність забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування;

– визначити досвід країн партнерів, що забезпечать швидкий, зручний та надійний спосіб забезпечення кібербезпеки інформаційних ресурсів між різнорівневими органами управління та самоврядування в Україні, щодо завдання кіберзахисту;

– дослідити напрями забезпечення кібербезпеки у Європі, США та України;

– визначити можливості удосконалення нормативно-правової складової у сфері кібербезпеки інформаційних ресурсів;

– розробити пропозиції у сфері кібербезпеки та перспектив подальших напрямів кібербезпеки.

**Методологія дослідження.** Для досягнення поставленої мети в роботі використано ряд загальнонаукових і спеціальних методів дослідження, які взаємопов'язані між собою та застосовувалися у роботі у послідовному і логічному зв'язку: порівняльно-історичний; метод структурно-логічного аналізу; метод аналізу та синтезу; методи порівняння, узагальнення, класифікації інформації при дослідженні закордонного досвіду; методи

систематизації та формалізації інформації для характеристики та аналізу сучасного стану реформування у сфері кібербезпеки інформаційних ресурсів органів управління та самоврядування в Україні.

**Практичне значення** одержаних результатів полягає у можливості їх використання при розгортанні організаційної й практичної діяльності у сфері кібербезпеки інформаційних ресурсів органів державного управління та самоврядування в Україні. Частина дослідницького матеріалу може використовуватись у навчальних програмах для підвищення кваліфікації державних службовців у сфері кібербезпеки.

**Структура і обсяг роботи**. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 70 сторінок. Список використаних джерел налічує 65 найменувань.

# РОЗДІЛ 1
# ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПУБЛІЧНОМУ УПРАВЛІННІ В УМОВАХ ЦИФРОВІЗАЦІЇ

## 1.1. Інформаційне забезпечення органів публічного управління в умовах цифрової трансформації публічного управління

Інформаційне забезпечення органів публічного управління в умовах цифрової трансформації публічного управління набуває нового значення і тісно пов’язане з питаннями захисту інформації та забезпечення кібербезпеки.

Введена в дію указом Президента України №447/2021 від 14 травня 2021 року "Про Стратегію кібербезпеки України" являє собою базовий документ, що дозволяє почати узгоджену роботу зі створення системи кібербезпеки в Україні. Проте успішному виконанню цієї роботи явно не сприятиме відсутність єдиної термінології у цій сфері, невизначеність ряду понять, які згадуються в стратегії кібербезпеки, зокрема таких базових понять, як кіберпростір, кібербезпека, кібернетична загроза і т.п. На поточний момент у сфері інформаційної безпеки стрімко зростає кількість публікацій з термінологічної тематики, що цілком зрозуміло, зважаючи на актуальність цієї проблеми. Існують різні підходи до її дослідження, причому аналіз змісту публікацій свідчить про іноді абсолютно суперечливе розуміння фахівцями основних термінологічних питань. В цій ситуації для успішного формування загальних уявлень про зміст та базові визначення у сфері кібербезпеки видається доцільним переглянути певні історичні події та факти, пов’язані з процесами виникнення і розвинення інформаційного та кіберпротиборства [1; 2; 3].

Насамперед розтлумачимо загальні поняття у забезпеченні кібернетичної безпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування таких, як:

Кібербезпека (кібернетична безпека) – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за

якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кіберпростір – це комплексне віртуальне середовище, що не має фізичного втілення, сформоване в результаті діяльності людей, програм і сервісів в мережі Інтернет шляхом мережних і комунікаційних технологій.

Кіберзлочинність – це загальна назва кримінальної діяльності, яку використовують на інтернет-просторах, часто з намірами заробити грошей або дістати особисту інформаці, також це являє собою сукупністю кіберзлочинів..

Кібершпигунство або комп’ютерний шпіонаж (вживається також термін «кіберрозвідка») – термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп’ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи «троянських коней» і шпигунських програм . Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп’ютери і комп’ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами. З недавніх пір кібершпигунство включає також аналіз провідними спецслужбами зокрема за спостереженням цифрового сліду поведінки користувачів соціальних мереж та месенджерів, таких як Facebook, Telegram, Twitter тощо з метою виявлення екстремістської, терористичної чи антиурядової діяльності, закликів збору на мітинги проти влади

Кібертероризм – під цим поняттям розуміють навмисну мотивовану атаку на інформацію, що обробляється комп’ютером, комп’ютерну систему або

мережу, яка пов’язана з небезпекою для життя і здоров’я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту, саме це сталося напередодні 24 лютого 2022 року коли країна агрессор розпочала військовий наступ на територію України.

Інформаційний ресурс – це, перш за все, джерело відповідним чином організованої інформації, ресурс у вигляді запасу, який можна використати в разі потреби, засіб, можливість, якими можна скористатися в разі необхідності. Це доступні для використання відомості в усіх сферах життєдіяльності людини, суспільства і держави, які зберігаються на відповідних носіях як документи, бази даних і знань, реєстри, кадастри та інші відомості, що можуть бути власністю будь-якого суб’єкта інформаційних відносин та бути залученими до обігу.

Публічне управління – це система яка складається з державних, місцевих, некомерційних структур, які створюються з метою задоволення суспільних інтересів та вирішення колективних проблем Воно спирається на державну владу, підкріплюється і забезпечується нею, також поширюється на все суспільство і за його межі у сфері проведення державної міжнародної політикиа, а саме держава шляхом законодавчої діяльності встановлює основні, загальні й типові правила поведінки людей та діє системно та неперервно, поєднуючи функціонування таких структур, як механізм держави, державний апарат, державну службу.

Організуючий і регулюючий вплив держави визначає суспільну життєдіяльність людей з метою її впорядкування, збереження чи перетворення, опираючись на владну силу, яку обмежує дієвий суспільний контроль.

Для протидії загрозам системі державного управління і мінімізації їх впливу на органи публічного управління та місцевого самоврядування України необхідно, насамперед, провести їх аналіз і оцінку. Існуючі підходи до оцінки зазначених загроз не передбачають їх комплексного розгляду за інформаційним, кібернетичним та корупційним напрямами.

Сучасні цифрові технології дозволяють використовувати сучасні методи та засоби обробки інформації в державному управлінні та висувають нові вимоги та очікування до державного сектору. Цифровізація – це впровадження цифрових технологій в усіх сферах життя суспільства. Це один із головних факторів зростання світової економіки та розвитку публічного управління в країнах світу.

Актуальність вивчення цього питання полягає в тому, що для глибоких, системних та докорінних змін, що сприятимуть розвитку України як країни з цифровою економікою, важливого значення набуває саме готовність до впровадження діджиталізованого публічного управління та формування цифрових компетентностей передусім у державних службовців, які надають публічні послуги.

Важливу роль в розвитку держави відіграє цифрова трансформація публічного управління, головним фактором якої є інформація та знання, шляхи доступу до них. В сучасних умовах цифрова трансформація публічного управління необхідна для забезпечення швидкої та якісної роботи органів державного управління. Ефективна цифрова трансформація передбачає залучення органів державної влади та місцевого самоврядування, відповідальних за впровадження державної політики в усіх сферах суспільних відносин [3; 4].

Цифровізація є ключовим фактором здорового розвитку 66 інформаційного суспільства та дозволяє підвищити ефективність роботи державного сектору і конкурентоспроможність країни. Цифровізація – це створення високої доданої вартості для держави, підвищення ефективності економіки та бізнесу

Як приклад цифрової трансформації є додаток «Дія» це також є одним з найважливіших кроків на шляху до інформатизації суспільства. Тут можна зареєструвати паспорт, реєстраційний номер облікової картки платника податків, свідоцтво, водійське посвідчення, студентський квиток, військовий квиток, закордонний паспорт тощо. Також можна скористатися різноманітними

послугами, які насамперед полегшуть роботу держслужбовців у органах публічного управління.

Одним з основних викликів в Україні є незахищеність відкритих даних, даних про особу. На жаль в Україні недостатньо унормована нормативно-правова база, де є деякі невизначені поняття, розбіжності. Не створено систему заходів для захисту відкритих даних про особу.

Прикладом цього є витік даних в додатку «Дія». Багато користувачів навіть не здогадувалися що дані були оброблені іншими особами на які користувачі не давали згоди. Тому варто робити заходи щодо захисту даних, де фактично кожен додаток який розробляється для надання послуг чи інших цілей, кожен проект супроводжується актом в якому вказується основні заходи щодо забезпечення конфіденційності особи.

Таким чином, цифровізація публічного управління в Україні реалізується на основі розробки і використання різних інформаційних систем, за допомогою яких відбувається розширення можливостей в прискореному режимі обробляти значні масиви інформації.

Дані системи дозволяють підтримувати систематизувати й упорядкувати різноспрямовані інформаційні потоки, які підтримуються в структурі надання та споживання державних послуг при всебічному результативності та ефективності їх, а також ступеня доцільності та продуктивності використання державних фінансових коштів.

При чіткому структурному функціонуванні позначених інформаційних систем створюється єдиний електронно-цифровий простір, якому потрібне забезпечення кібербезпеки інформаційних ресурсів в органах публічного управління та місцевого самоврядування [6 ; 7].

Цифрова трансформація сьогодні є об’єктивним процесом, що заповнює всі сфери соціального існування, у тому числі діяльності в секторі публічного управління та місцевого самоврядування.

Нове цифрове середовище дозволить не тільки накопичувати необхідні дані про життя і події в суспільстві й за кордоном у базах даних і знань, в

експертних системах, а й використовувати їх у потрібний час, у потрібній формі для вирішення нагальних завдань і проблем.

За своїм змістом «концепція» – це певний спосіб розуміння, трактування будь-якого предмета, явища, процесу та інше, керівна ідея для їх систематичного висвітлення.

Розуміння концепції цифрової безпеки можливо пояснити, як цифрову безпеку також відому як кібербезпека, яка сьогодні стає все більш важливою в органах державної влади, захищає фізичну та цифрову інфраструктуру, пов'язану з технологіями, і забезпечує рівень захисту цифрової інформації [5; 8].

Існує ряд інструментів і методів, доступних для захисту органів державної влади від кібератак, хоча ситуація постійно змінюється. Ось деякі з найпоширеніших загроз цифровій безпеці:

- Кіберзлочинність відбувається постійно особливо в умовах війни у 2022 році, використовуючи незаконні канали та крадіжку паролів, «хакери» отримують доступ до цінної інформації від окремих осіб які працюють в органах публічного управління та місцевого самоврядування і прагнуть отримати як прибуток від злочинної поведінки так нанести збитки нашій державі.

Часто атаки можуть призвести до втрати контролю над обладнанням або пристроями, і хакери прагнуть отримати більше даних у власників в обмін на відновлення контролю.

- Також у тепершніх умовах війни кібертероризм являє собою незаконне використання програмного забезпечення для викрадення або перехоплення інформації та використання цієї інформації для навіювання страху іншим, будь то громадськість, окремі особи чи уряди.

Загалом ці атаки мають за собою політичні наміри з метою перехопити інформацію, яка може скомпрометувати політичну партію, уряд чи особу. Було кілька випадків витоку конфіденційної інформації.

Захист даних та інформації життєво важливий для огранів державної влади і важливий для захисту держави. Для ефективної та безпечної роботи необхідно навчити держслужбовців дотримуватися безпечних процесів і використовувати системи цифрової безпеки, які можуть забезпечити захист від загроз кібербезпеці та дій.

Загрози цифровій безпеці можуть бути спричинені:

- Віруси та шкідливі програми, створені для створення проблем, наприклад трояни.
- Помилки програмування, які можуть бути використані третіми особами для підозрілих цілей.
- Цифрові зловмисники або люди, яким вдалося ввести дані несанкціонованим способом.
- Збитки, такі як крадіжки, повені, пожежі або втрата матеріалів, файлів або пристроїв.

Сучасні органи публічного управління стикаються з загрозою зовнішніх атак, яких просто не існувало багато років тому. Розвиток Інтернету збільшив ризик, і дані стали цінним активом особливо коли держава агресор цілеспрямовано націлена на них.

Виділяють 5 найпоширеніших кібератак:

- Шпигунське програмне забезпечення це шкідлива програма має на меті атакувати та викрадати інформацію; потім дані передаються зовнішній особі без відома або згоди власника.

Згубний вірус може послабити й потенційно зруйнувати структуру орган державної влади. Зазвичай метою атаки є отримання даних з ціллю знищення інфраструктурного об’єкту, та опублікуванні даних з метою залякування та дезінформації населення.

- Програми-вимагачі – це дуже шкідливе програмне забезпечення, яке захоплює дані та може обмежувати доступ до ключових областей операційної системи. Він забороняє користувачам доступ до пристрою, і щоб вирішити проблему, потрібно заплатити викуп за звільнення пристрою, що

може повести за собою втрату даних державного рівня, силами самого користувача.

Програми-вимагачі поширюються через троянів або хробаків, які можуть скористатися будь-якою вразливістю операційної системи.

- Рекламне програмне забезпечення – це програмне забезпечення, призначене для відображення реклами для залучення державних працівників та громадян України на погляди притаманні державі агресору.

Це може бути критично для нашої держави, оскільки інформацію отримують із реклами, з якою консультуються користувачі.

Рекламне програмне забезпечення не є вірусоподібним троянським програмам або хробаком, але може негативно впливати на роботу органів влади.

- Фішинг поширюється електронною поштою і може швидко поширюватися; простий електронний лист може повідомити одержувачу, що йому потрібна інформація для завершення чи продовження процесу або що він щось виграв, або бути підробкою листа від іншої державної установи.

Електронний лист зазвичай містить посилання, яке спрямовує людей на цільову сторінку, схожу на справжню. Заповнюючи запитувані дані, користувачі фактично діляться цими даними з кіберзлочинцями, які використовують їх неправомірно.

- Відмова в обслуговуванні (DOS) - зловмисники можуть робити кілька запитів на сервер, доки він не зможе їх обслуговувати, саме це сталося на всі інформаційні ресурси України напередодні 24 лютого 2022 року коли країна агресор розпочала військове вторгнення на територію нашої держави.

Це можна зробити двома способами:

1. Відмова в обслуговуванні або DoS: використовується одна IP-адреса або комп’ютер, який послідовно запускає незліченну кількість підключень до атакованого сервера.

2. Відмова в обслуговуванні або DDoS: у цьому методі використовується кілька різних комп’ютерів або IP-адрес, які надсилають багато запитів серверу, доки його не заблокують.

Слід відзначити, що безпека в цифровому світі має багато форм, які пропонують широкий вибір методів захисту.

## 1.2. Основні напрямки забезпечення інформаційної безпеки в цифровому суспільстві

Рівень розвитку та безпека інформаційного середовища, які є одними з найвагоміших факторів у всіх сферах державної безпеки, активно впливають на стан політичної, економічної та інших складових державної безпеки України. У зв'язку з цим доцільно розглядати інформаційну безпеку як складову інших сфер державної безпеки. Разом з цим, інформаційна безпека є самостійною складовою державної безпеки і в цьому проявляється її двоїстий характер. Це обумовлюється таким:

– прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів;

– необхідністю не лише розвивати й посилювати національний інформаційний потенціал, але й захищати від широкого спектра існуючих і потенційних інформаційних загроз;

– існуванням реальної потреби в захисті всіх суб'єктів інформаційних відносин від можливих негативних наслідків упровадження та використання інформаційних технологій;

– наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою одержання односторонніх переваг в політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість індивідів, на сім'ю, суспільство й державу, що загрожує державній безпеці [8, с. 87].

Однією з головних проблем забезпечення інформаційної безпеки є відсутність усталеного поняття «інформаційна безпека».

Аналіз літератури з проблематики дає підстави зазначити, що поняття «інформаційна безпека» розглядається з різних ракурсів. Наведено деякі з них, так інформаційна безпека – це:

- стан захищеності інформаційного середовища, який відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційний загроз» [2, с. 101];
- стан інформаційного середовища суспільства і політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства[10, с. 128];
- стан захищеності інформації, яка забезпечує життєво важливі інтереси людини [13]. В межах цього методологічного напряму використовується визначення інформаційної безпеки як стану, тенденцій розвитку, умов життєдіяльності соціуму, його структури, інститутів та установ, за яких забезпечується збереження якісної інформації з об'єктивно обумовленими інноваціями в ній, вільне і відповідне власній природі її функціонування;
- відсутність небезпеки, тобто тих чинників та умов, які загрожують безпосередньо індивіду, державі, спільноті з боку інформаційно-комунікаційного середовища. Дослідники, які додержуються таких підходів, під інформаційною безпекою розуміють стан та процес захищеності особи, суспільства, держави від реальних або потенційних загроз [14, с. 34];
- інформаційний компонент національної безпеки по співвідношенню «частина-ціле» [9, с. 132]. Цей дослідник характеризує національну безпеку як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови існування людини, держави і суспільства, які гарантовані Конституцією та законами України;
- це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [15].

Інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека

визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Наукові дослідження не виробили загальноприйнятого механізму структуризації забезпечення інформаційної безпеки. Для виокремлення складових його загальної структури найчастіше використовуються такі конструкції, як «напрями», «механізми» та «шляхи» забезпечення [13].

На нашу думку, інформаційна безпека в системі публічного управління – є складовою національної безпеки України, яка забезпечую захист системи публічного управління від інформаційно-комунікаційних загроз та викликів, у той же час сама система публічного управління забезпечує суспільство, державу та громадян інформаційно-якісними послугами та якісною інформацією. Тобто система інформаційної безпеки носить двосторонній характер: зовнішній та внутрішні, тобто захищає себе та захищає інших від неякісної інформації, інформаційних атак тощо.

Наступною проблемою є відсутність дієвих механізмів забезпечення інформаційної безпеки. Так, відповідно до Доктрини інформаційної безпеки України [6] актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [6].

Водночас, на сьогодні не створена єдина система забезпечення інформаційної безпеки публічного управління.

Наступна проблема, це забезпечення підготовки якісного кадрового складу систему публічного управління у сфері забезпечення інформаційної безпеки. Людський ресурс – є основою у прийнятті та реалізації будь-яких управлінських рішень, тому потребує вирішення на державному рівні формування нового складу державних службовців, які вирішуватимуть проблеми забезпечення інформаційної безпеки системи публічного управління.

Ще одна проблема – це забезпечення дієвого механізму функціонування систему електронного врядування, яка, на даний час, на жаль, не діє. Існують розроблені системи електронного документообігу в органах державної влади та органах місцевого самоврядування, однак єдиної системи електронного врядування в Україні не існує.

Наступна проблема – це формування інноваційних інформаційних небезпек, які потребують термінового та ефективного вирішення. Розвиток та

впровадження в різні сфери життя суспільства новітніх інформаційних технологій, як і будь-яких інших науково-технічних досягнень, не тільки забезпечує комфортність, але й нерідко несе певну небезпеку. Зокрема загальними є групи інформаційно-технічних небезпек:

- новий клас соціальних злочинів направлений проти особистості, суспільства, держави, заснований у використанні сучасної інформаційної технології (кібертероризм і кіберзлочинність: махінації з електронними грошима, комп'ютерне хуліганство та інші);

- використання нових інформаційних технологій в політичних цілях;

- електронний контроль за життям, планами громадян, політичних організацій;

- бурхливий розвиток нового класу зброї - інформаційної, яка здатна ефективно впливати на психіку та свідомість людей, на інформаційно-технічну інфраструктуру суспільства і армії [1; 13-15].

Ще однак проблема – відсутність інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в публічному управлінні. Відповідно до Закону України «Про національну безпеку» до складу сектору безпеки і оборони входять: Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику. Інші державні органи та органи місцевого самоврядування здійснюють свої функції із забезпечення національної безпеки у взаємодії з органами, які входять до складу сектору безпеки і оборони [7]. Водночас, не

визначено взаємозв’язок зазначених органів в системі забезпечення інформаційної безпеки, у тому числі у сфері публічного управління.

На нашу думку, потребує розробка та реалізація Закону України «Про забезпечення інформаційної безпеки України», де потрібно визначити також органи державної влади, які реалізуватимуть державну політику у сфері інформаційної безпеки.

Основними напрямками забезпечення цифрової безпеки є забезпечення наявність процедур цифрової безпеки, аналізу та перевірок. Їм також може знадобитися провести моделювання для різних типів подій і якими будуть процеси вирішення. Цей аналіз може включати:

- Комунікації.
- Планування.
- Контроль ризиків.
- Додатки для органів публічного управління та місцевого самоврядування.
- Обслуговування громадян.
- Системи та інфраструктура.

Для забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування насамеред повині буті розроблені процедури та план тестування та переконатися, що інші державні органи дотримуються протоколу цифрової безпеки. Щоб бути захищеними від атак або загроз, органи управління, операцій, фінансів і зв’язку повинні пройти навчання щодо рекомендованих процесів і завдань для захисту даних держави.

Нижче наведено кілька основних кроків, які виконуються на даний час, щоб встановити процедури обробки даних і захисту державних активів [10; 11; 12; 13]:

- Навчання керівників і співробітників - стандарти та процедури безпеки повинні бути доведені до відома кожного співробітника, щоб забезпечити правильну обробку інформації. Наприклад на порталі дія цифрова освіта (https://osvita.diia.gov.ua/) є можливість кожному пройти курси з базових

заходів кібернетичної безпеки, та отримати сертифікат для підтвердження своїх знань для представлення його у органах публічного управління та місцевого самоврядування задля допуску співробітників до інформаційних ресурсів цієї сфери.

- Впровадження програмного та апаратного забезпечення безпеки - оптимізує процес цифрової безпеки для даних органів в безпечній системі. Усі технологічні пристрої повинні бути оснащені антивірусними та антишпигунськими програмами, щоб забезпечити захисний бар'єр від шкідливого програмного забезпечення.
- Розвиток корпоративної культури та політик безпеки - захист кращий, ніж боротьба з порушенням системи безпеки, тому потрібно бути переконаним, що передові цифрові практики впроваджені в корпоративну культуру та політику. Такий підхід допоможе уникнути витоків або доступу зловмисників.
- Розуміння існуючих ризиків- такі ризики, як шахрайство, корпоративне шпигунство, викрадення облікових даних та інші зловмисні дії, можуть вплинути шкідливо вплинути державні органи. Якщо у вас є одна людина, яка натискає шкідливе посилання з новим і невідомим вірусом, усе може розвалитися. Важливо визначити доступ і права кожного співробітника або партнера державного органу.
- Розгорнуті віртуальні приватні мережі або VPN – це послуга, яка забезпечує віддалений доступ до внутрішньої мережі державних органів та різних бізнес-ресурсів, таких як сервери електронної пошти, презентації та настільні програми. VPN-мережа забезпечує безпечний доступ через Інтернет для віддалених працівників і тих, хто перебуває в інших місцях. Він створює безпечне шифрування для доступу держслужбовців до послуг і документів з будь-якого місця. Підключення до корпоративної мережі без VPN може загрожувати цифровій безпеці.

Ці дії забезпечують кібербезпеку інформаційних ресурсів органів публічного управління та місцевого самоврядування, якщо всі конфіденційні

бізнес-дані захищені від зловмисних намірів. Важливо створювати культуру цифрової безпеки та динаміку роботи, яка вивчає та контролює ці аспекти [14].

Сучасне забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування є складною системою з великою кількістю підсистем різного функціонального призначення, які потребують якісного управління на різних ланках з реалізацією автоматизованим (для вищих рівнів) або автоматичним (бажано для нижчого рівня) способом.

Вимоги до пропозицій та перспектив в даній сфері-сукупність тверджень щодо атрибутів, властивостей або якостей захисту інформаційних ресурсів, що підлягає реалізації.

Таким чином, пропозиції та перспективи повинні оптимізувати забезпечення кібербезпеки інформаційних ресурсів даних органів з необмеженою кількістю, як державних службовців так і громадян України, трафік від яких, надходить на дані ресурси.

В ході подальшого формулювання завдання і дослідження предметної області, з урахуванням економічних і тимчасових вкладень було проведено уточнення завдання.

Дані пропозиції та перспективи повинні задовольняти наступним вимогам:

- мінімальні вимоги до апаратних ресурсів;
- відкритість інформації без можливості нанести шкоду;
- розширюваність і масштабованість;
- продуктивність та надійність;
- сумісність, керованість та захищеність;
- стандартні засоби надання діагностичної інформації;
- наявність докладної документації на всю використовувану нормативно-правову базу;
- здатність працювати з обладнанням різних виробників.

Таким чином, постановка задачі має вид:

Реалізувати пропозиції та перспективи для забезпечення кібербезпеки інформаційних ресурсів в органах публічного управління та місцевого самоврядування за даними вимогами:

- Вибір нормативно-правової бази;
- вибір технологій для вирішення задачі;
- вибір апаратного забезпечення для вирішення задачі;
- моделювання системи захисту інформаційних ресурсів;
- реалізація пропозицій захисту в умовах війни;
- перспективи адаптування захисту у майбутьому з урахуванням досвіду країн партнерів.

Потрібно здійснити реалізацію пропозицій та перспектив забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування на основі сучасної нормативно-правової бази та досвіду країн партнерів в умовах українсько-російської війни від 2014 року по теперішній час, а саме максимально адаптувати сучасні рішення та можливості додавання нових в процесі війни [15; 16; 17; 18].

Кібернетична безпека – стан захищеності критичних об’єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави. В сучасних умовах для підвищення ефективності організації та виконання запланованих робіт крім наявного ресурсу необхідно застосовувати інформаційні технології, які можуть сприяти своєчасному, адекватному, повному і прихованому виконанню певного класу завдань забезпечення кібербезпеки інформаційних ресурсів.

Реалізація пропозицій та перспектив забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування є прикладом зручного використання в системі управління державного призначення, яка є простою у користуванні та освоєнні та відповідає сучасним вимогам нормативно-правової бази України.

Використання інформаційних технологій дозволить зменшити часові затрати на процес захисту від кібератак та підвищити продуктивність роботи інформаційних ресурсів відповідних органів та захисту в цілому.

# РОЗДІЛ 2
# СВІТОВИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1. Досвід забезпечення інформаційної безпеки від кіберзагроз в США та Європі.

Світовий досвід вказує на те, що забезпечення можливостей у галузі забезпечення кібернетичної безпеки, де близько 70 країн світу на сьогодні активно займаються питаннями кібербезпеки в органах державної влади, в тому числі у військовій сфері. Близько 50 країн мають власні системи кібербезпеки, які створені за останнє десятиріччя [19; 20; 21; 22].

У сучасних умовах питання забезпечення кібербезпеки не обмежуються лише організацією системи захисту інформації на окремому об’єкті критичної інформаційної інфраструктури, а й передбачають створення єдиної системи захисту кібернетичного простору як складової частини інформаційної та національної безпеки будь-якої держави світу.

У даному розділі визначено стратегічні основи міжнародного співробітництва України у сфері кібербезпеки. Узагальнено завдання міжнародної взаємодії у сфері кібербезпеки. Проаналізовано міжнародні ініціативи, які впроваджуються з метою посилення захисту кіберпростору. Деталізовано напрямки здійснення модернізації політики інформаційної безпеки на рівні ООН. Окреслено ключові пріоритети міжнародного співробітництва у сфері забезпечення кібербезпеки між Україною та НАТО. Розглянуто перспективи діяльності в Україні Трастового фонду з кібербезпеки НАТО. Обґрунтовані сучасні світові тенденції, які впливають на безпекову політику НАТО і вимагають вжиття відповідних заходів реагування. На підставі узагальнення визначено шляхи удосконалення міжнародної співпраці у сфері забезпечення кібербезпеки.

Нині більшість держав світу успішно проводять політику посилення кібербезпеки та її складників. У міжнародному форматі можна виділити три основні моделі правового врегулювання поширення інформації:

Перша модель передбачає тотальний, жорсткий контроль держави над мережею Інтернет. Такої моделі дотримується, наприклад, КНР, де практично весь Інтернет перебуває під повним державним контролем. Окремі елементи китайського досвіду сьогодні впроваджуються в практичну площину в країні-агресорі РФ.

Друга модель передбачає відповідальність провайдера за будь-які дії користувача. Наприклад, у Франції провайдери зобов'язані надавати відомості про авторів сайтів на вимогу третіх осіб. Крім того, у Франції ще з 1978 року існує спеціальний орган (Національна комісія інформатики і свобод), який зобов'язаний контролювати, щоб інформація в мережі не порушувала права і свободи людини.

Третя модель регулювання безпеки в мережі Інтернет передбачає звільнення провайдера від відповідальності в тому разі, якщо він виконує певні умови, пов'язані з характером надання послуг і взаємодії із суб'єктами інформаційного обміну. Так, у Німеччині відповідальність провайдерів за розміщення нелегального контенту на Інтернет-ресурсах, що знаходяться в їх мережі, настає лише в разі, якщо вони самі є власником інформації або свідомо поширювали її з посиланням на інші джерела. Така модель також активно використовується в Японії.

За таких умов можна констатувати, що кожна країна світу вибирає власну модель розбудови національної системи кібербезпеки.

Досвід забезпечення кібернетичної безпеки в США: Російсько-українська війна, що точиться на українській землі, – це випробування всіх матеріальних і духовних сил нашого народу та війська. На сьогодні проблема захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, від викликів і загроз у кібернетичному просторі є однією з найголовніших для будь-якої держави, а забезпечення належного рівня кібернетичної безпеки

держави є необхідною умовою забезпечення національної безпеки держави, розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем державного управління та захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи державного управління кібернетичною безпекою – як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам.

В умовах російсько-української війни відбуваються зміни, які стосуються функціонування кібернетичної безпеки в Україні, відповідно до конкретних умов здійснюються певні кроки, спрямовані на зміцнення обороноздатності країни з допомогою країн партнерів та обміну досвідом з інформаційною базою в цій галузі з США [23].

Аналіз законодавства США у сфері кібернетичної безпеки: Сьогодні законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів та законів штатів, які створили правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це насамперед, такі закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп’ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп’ютерних систем» (1987 р.). Широкими принципами є: правова, організаційна та фінансова автономія органів місцевого самоврядування[1; 24; 25].

Секретна служба США підтримує цільові групи, які зосереджені на виявленні та пошуку міжнародних кіберзлочинців, пов’язаних із кібератаками, банківським шахрайством й іншими комп’ютерними злочинами. Відділ кіберрозвідки Секретної служби безпосередньо сприяє арештам транснаціональних кіберзлочинців, відповідальних за крадіжку сотень мільйонів номерів кредитних карт і втрату близько 600 млн дол фінансовими й роздрібними установами. Секретна служба також керує Національним комп’ютерним криміналістичним інститутом, який надає працівникам правоохоронних органів, прокурорам та суддям кіберпідготовку та інформацію для боротьби з кіберзлочинністю.

Аналіз законодавства США у сфері інформаційної безпеки показує, що основними напрямами забезпечення національної кібербезпеки США є захист критично важливих об’єктів інфраструктури, а саме – їх інформаційних систем від кібернетичних атак; вдосконалення засобів виявлення таких атак і оперативного реагування на них; визначення завдань безпеки кіберпростору та способи їх вирішення; підготовка відповідних фахівців з безпеки інформації та взаємодія з приватним сектором; співпраця з міжнародними організаціями з метою забезпечення відкритого, безпечного, надійного кіберпростору[3; 26].

У свою чергу США мають величезний досвід у сфері впровадження інформаційних технологій в діяльність держави з усіх напрямів. Особливо важливим, в умовах військового захисту Україною своїх територій у відповідь на збройну агресію іноземної держави, є американський досвід використання інформаційних технологій для створення систем зв’язку та військового управління, а також високоточного озброєння.

Реагування на інциденти кібернетичної безпеки в США: NCSD фінансується за рахунок наступних трьох програм, проектів і заходів, затверджених Конгресом: Комп'ютерна команда екстреної готовності США (US-CERT), Стратегічні ініціативи:

US-CERT використовує компетенції аналітичних центрів для формування бази знань і практик у сфері кібербезпеки. US-CERT являє собою єдиний центр

підтримки федеральної влади у сфері підготовки рішень по забезпеченню захисту цивільних комп'ютерних мереж федеральної виконавчої влади. US-CERT здійснює аналіз загроз і вразливостей, поширює інформацію про можливі кіберзагрози, координує свою діяльність з партнерами і клієнтами для досягнення загальної поінформованості про стан кіберінфраструктури країни [4; 28].

Реагування на інциденти – це структурований процес, який організації використовують для виявлення та усунення інцидентів кібербезпеки. Реагування включає кілька етапів, включаючи підготовку до інцидентів, виявлення та аналіз інциденту безпеки, локалізацію, ліквідацію та повне відновлення, а також аналіз і навчання після інциденту.

Чотири етапи реагування на інциденти NIST в США [4; 5]:

1. Підготовка - щоб підготуватися до інцидентів, складіть список IT-активів, таких як мережі, сервери та кінцеві точки, визначивши їхню важливість і те, які з них є критичними або містять конфіденційні дані. Налаштуйте моніторинг, щоб у вас була базова норма нормальної діяльності. Визначте, які типи подій безпеки слід досліджувати, і створіть детальні кроки реагування на поширені типи інцидентів.

2. Виявлення та аналіз - виявлення передбачає збір даних з IT-систем, інструментів безпеки, загальнодоступної інформації та людей всередині та за межами організації, а також ідентифікацію провісників (ознаки того, що інцидент може статися в майбутньому) та індикаторів (дані, які показують, що атака сталася або відбувається зараз ).Аналіз передбачає визначення базової або нормальної активності для постраждалих систем, кореляцію пов’язаних подій і визначення того, чи відхиляються вони від нормальної поведінки.

3. Стримування, ліквідація та відновлення - мета стримування це зупинити атаку до того, як вона перевантажить ресурси або завдасть шкоди. Така стратегія стримування залежатиме від рівня шкоди, яку може спричинити інцидент, необхідності підтримувати доступність критично важливих послуг

для співробітників і клієнтів, а також тривалості рішення - тимчасове рішення на кілька годин, днів або тижнів або постійне рішення.

4. Діяльність після інциденту - основною частиною методології реагування на інциденти NIST є вивчення попередніх інцидентів для покращення процесу.

Використання своїх висновків, щоб покращити процес, скорегувати свою політику, план і процедури реагування на інциденти та передати нові дані на підготовчий етап процесу реагування на інциденти.

Узагальнення здобутків США у сфері забезпечення кібербезпеки: Проаналізовано п’ять основних напрямів діяльності з питань інформаційного захисту, які визначає Стратегія: постійний моніторинг і безперервна оцінка загроз та вразливих місць державних інформаційних систем; здійснення національних заходів зі зменшення загроз й уразливості кіберпростору; уживання заходів щодо захисту інформаційних систем органів влади; забезпечення якісної освіти та навчання з питань захисту кіберпростору; співробітництво з питань національної безпеки й безпеки міжнародного кіберпростору [6].

У ході дослідження виявлено такі чинники, що сприяли проведенню успішної інформаційної політики США:

– нормативно-правове регулювання;

– державні органи;

– інформованість та довіра населення;

– кіберстрахуваня.

Нормативно-правове регулювання – чи не найголовніший двигун ефективності забезпечення інформаційної безпеки будь-якої держави. Американський уряд значну увагу приділяв питанням забезпечення безпеки інформації в державних комп’ютерних системах (закони США «Про комп’ютерну безпеку» та «Про удосконалення інформаційної безпеки»), протидії комп’ютерній злочинності (закони «Про комп’ютерне шахрайство та зловживання» і «Про зловживання комп’ютерами»), регулювання

співвідношення прав громадян на отримання інформації (закони «Про свободу інформації» та «Про висвітлення діяльності уряду») та конфіденційності їхнього приватного життя (закон «Про охорону персональних даних») [7].

Державні структури відіграють важливу роль у забезпеченні інформаційної безпеки. Структура інформаційної безпеки в США є доволі розгалуженою та включає в себе значну кількість компонентів, на кожен із яких покладено відповідні завдання та функції з урахуванням їх компетенції.

Довіра та обізнаність населення. Незважаючи на кібератаки, населення, зазвичай, продовжує довіряти установам, які впорядковують дані та особисту інформацію в мережі Інтернет. Проте близько 53 % споживачів втратили довіру до свого уряду [8]. Американці прагнуть до цифрової грамотності й бажання її покращити виходить далеко за рамки молодого покоління. Більше восьми з 10 опитаних людей сказали, що хочуть поліпшити свої знання й уміння в цій сфері. Загальні мотиватори для бажання покращити навички цифрової грамотності включають заощадження грошей, інформування й підтримку друзів та сім'ї.

Кібер-страхування – захист малого та середнього бізнесу. Кібер-страхування – це страховий продукт, що використовується для захисту бізнесу й окремих користувачів від ризиків, пов'язаних з Інтернетом і в цілому ризиків, пов'язаних з інфраструктурою та діяльністю в галузі інформаційних технологій. Атаки на весь бізнес зростають. Малі підприємства схиляються до думки, що їх ця загроза омине, проте Symantec виявив, що понад 30 % випадків фішингу у 2015 р. простежено в організаціях із 250 працівників. Звіт Symantec про загрози Інтернет-безпеці у 2016 р. засвідчив, що 43 % усіх атак у 2015 р. були спрямовані на малі підприємства [9].

Досвід забезпечення кібернетичної безпеки у Європі: Поширення популярності цифрової економіки як принципово нової моделі розвитку глобальної економічної системи постійно зростає, що провокує необхідність розробки дієвих механізмів забезпечення надійного та безпечного середовища її функціонування. Прагнення політичного керівництва держав світу

зміцнювати та посилювати систему забезпечення кібербезпеки нерозривно пов’язано із реагуванням на реальні та потенційні загрози, що передбачає вдосконалення законодавства, визначення стратегічних засад подальшого розвитку у базових програмних документах та їх реалізації. Враховуючи прагнення України інтегруватися у європейський інформаційний простір, актуальним та своєчасним є огляд новел сучасного законодавства ЄС, зокрема оновленої Стратегії кібербезпеки, яка визначає поступальні та дієві кроки спільної європейської інформаційної політики з метою посилення спроможності держав-членів ЄС у сфері забезпечення кібербезпеки, захисту надбань цифрової економіки.

Метою є висвітлення й узагальнення кращих практик європейського досвіду щодо побудови та удосконалення системної протидії кіберзагрозам в сучасних умовах, проведення огляду новел європейського законодавства у сфері забезпечення кібербезпеки, зокрема Стратегії ЄС у вказаній сфері та висвітлення базових напрямків.

Аналіз стратегії кібербезпеки у Європі: Рада ЄС визначила ключові напрямки діяльності із розвитку кібернетичної безпеки на наступні роки. Серед них, зокрема, намір створити мережу оперативних центрів з безпеки по усьому ЄС, головним призначенням якої буде прогнозування, своєчасне виявлення та протидія кібернетичним атакам на комунікаційні мережі. При цьому в ЄС має бути визначена оперативна структура, яка буде опікуватися питаннями координації дій та кризового менеджменту для протидії кібернетичним атакам та загрозам.

Стратегія охоплює безпеку основних послуг, таких як лікарні, енергетичні мережі, залізниці та постійно зростаючу кількість підключених об’єктів у наших будинках, офісах і на заводах. Стратегія спрямована на створення колективних можливостей для реагування на великі кібератаки. Він також окреслює плани співпраці з партнерами по всьому світу для забезпечення міжнародної безпеки та стабільності в кіберпросторі. Крім того, у ньому описано, як Об’єднаний кіберпідрозділ може забезпечити найефективнішу

відповідь на кіберзагрози, використовуючи колективні ресурси та досвід, доступний державам-членам і ЄС [1].

Нова стратегія спрямована на забезпечення глобального та відкритого Інтернету з надійними гарантіями там, де існують ризики для безпеки та основних прав людей у Європі. Після прогресу, досягнутого в рамках попередніх стратегій, він містить конкретні пропозиції щодо застосування трьох основних інструментів. Ці три інструменти – це регуляторні, інвестиційні та політичні ініціативи. Вони стосуватимуться трьох сфер діяльності ЄС:

1 – стійкість, технологічний суверенітет і лідерство;

2 – оперативні можливості для запобігання, стримування та реагування;

3 – співробітництво для розвитку глобального та відкритого кіберпростору.

ЄС має намір підтримувати цю стратегію шляхом безпрецедентного рівня інвестицій у цифровий перехід ЄС протягом наступних семи років. Це збільшить попередній рівень інвестицій у чотири рази. Це демонструє відданість ЄС його новій технологічній та промисловій політиці та програмі відновлення.

Існуючі заходи на рівні ЄС, спрямовані на захист ключових послуг та інфраструктури від кібернетичних і фізичних ризиків, потребують оновлення. Ризики кібербезпеки продовжують розвиватися із зростанням цифровізації та взаємозв’язку. Фізичні ризики також стали складнішими після прийняття в 2008 році правил ЄС щодо критичної інфраструктури, які наразі охоплюють лише енергетичний і транспортний сектори. Перегляди спрямовані на оновлення правил відповідно до логіки стратегії Союзу безпеки ЄС, подолання хибної дихотомії між онлайн і офлайн і руйнування підходу ізоляції [2; 37;38; 39; 40].

Щоб відповісти на зростаючі загрози, спричинені цифровізацією та взаємозв’язком, запропонована Директива про заходи для високого загального рівня кібербезпеки в Союзі охоплюватиме середні та великі підприємства з більшої кількості секторів на основі їх критичності для економіки та

суспільства. NIS 2 посилює вимоги до безпеки, що висуваються до компаній, стосується безпеки ланцюгів постачання та взаємовідносин з постачальниками, спрощує зобов'язання щодо звітності, запроваджує більш суворі заходи нагляду для національних органів влади, суворіші вимоги до виконання та спрямований на гармонізацію режимів санкцій у державах-членах. Пропозиція NIS 2 допоможе збільшити обмін інформацією та співпрацю з управління кіберкризою на національному рівні та рівні ЄС.

Кібербезпека є одним із головних пріоритетів Комісії та наріжним каменем цифрової та пов'язаної Європи. Збільшення кількості кібератак під час коронавірусної кризи показало, наскільки важливо захищати лікарні, дослідницькі центри та іншу інфраструктуру. Потрібні рішучі дії в цій сфері, щоб забезпечити економіку та суспільство ЄС у майбутньому.

Реагування на інциденти кібернетичної безпеки у Європі: Комісія ЄС з кібербезпеки пропонує створити спільний кіберпідрозділ (JCU) для реагування на зростаючу кількість серйозних кіберінцидентів, які впливають на державні служби, підприємства та громадян у всьому Європейському Союзі [37;38].

Новий підрозділ кіберреагування об'єднає ресурси та досвід держав-членів Європейського Союзу для запобігання і реагування на інциденти безпеки. Він також включатиме приватні компанії, правоохоронні органи та інші спільноти кіберзахисту. Партнерство дозволить ЄС колективно реагувати та обмінюватися відповідною інформацією про кіберзагрози в ЄС [3].

Комісія ЄС з кібербезпеки заявляє, що створить підрозділ через поступовий і прозорий процес і дозволить спільне володіння з різними партнерами. Реагування на інциденти – це структурований процес, який організації використовують для виявлення та усунення інцидентів кібербезпеки. Реагування включає кілька етапів, включаючи підготовку до інцидентів, виявлення та аналіз інциденту безпеки, локалізацію, ліквідацію та повне відновлення, а також аналіз і навчання після інциденту.

ЄС також як і США використовують чотири етапи реагування на інциденти NIST.

Узагальнення здобутків Європи у сфері забезпечення кібербезпеки: 9 березня 2021 року Колегія Єврокомісії схвалила дорожню карту “Цифровий компас” [4, 5] – декларативний документ, який визначає перспективи та завдання у сфері розвитку глобальної цифрової трансформації до 2030 року. Як йдеться в документі, “Цифровий компас” відображає перспективи технологічного розвитку ЄС до 2030 року у чотирьох напрямах – цифрова освіта, цифрова інфраструктура, цифровий розвиток бізнесу, цифровий розвиток державного сектору.

Перший напрямок стосується цифрової освіти населення та підготовки досвідчених фахівців у сфері цифрових технологій. Це означає, що до 2030 року, 80 % усього населення ЄС повинні мати базові цифрові навички. При цьому в ЄС мають бути працевлаштовані не менше 20 мільйонів фахівців у цифровій сфері, серед яких має суттєво зрости доля зайнятості жінок.

Другий – передбачає розвиток безпечної, ефективної та захищеної цифрової інфраструктури. До 2030 року всі домогосподарства мають бути забезпечені комунікаціями гігабітного рівня, а всі населені регіони мають отримати покриття мережею 5G. На той час на Європу має припадати не менше 20 % світового обсягу виробництва напівпровідників, виробництво передових та стійких напівпровідників у Європі має становити 20 % світового виробництва. Передбачається створення не менше 10 тис. ефективних та екологічних передавальних вузлів [7, 8]. У Європі має з’явитися перший квантовий комп’ютер до 2025 року. До 2030 року очікується створення конкурентних європейських підприємств з повними циклами роботи щодо постачання напівпровідників – від проектування компонентів до готових продуктів. Центром суцільної цифровізації стануть промислові підприємства з виробництва процесорів формату 5G. Також планується значно знизити залежність від поставок цифрових продуктів з Південно-Східної Азії та Китаю

Третій – стосується цифрового розвитку для бізнесу. До 2030 року три з чотирьох компаній мають використовувати “хмарні” комп’ютерні послуги, бази “великих даних” та засоби штучного інтелекту. Очікується, що не менше 90 %

малих та середніх промислових підприємств мають досягти принаймні базового рівня інтенсивності у застосуванні комп'ютерних технологій.

Четвертий – цифровий розвиток державного сектору передбачає, що до 2030 року всі ключові громадські та соціальні послуги мають бути доступними у форматі онлайн. Громадяни ЄС зможуть повноцінно використовувати засоби цифрової ідентифікації, мати безобмежений доступ до власних електронних даних [6].

Таким чином, "Цифровий компас" ЄС являє собою звіт правил амбіційного та динамічного розвитку цифрової сфери та суцільної діджиталізації на поточні 10 років, а його практичне впровадження надасть змогу піднятися Євросоюзу у рейтингу світового технологічного розвитку на лідерські позиції, налагодити масштабне промислове виробництво напівпровідників та встановити контроль над 20 % світових поставок мікросхем та процесорів у цьому сегменті.

## 2.2. Порівняльний аналіз забезпечення інформаційної безпеки в США, Європі та Україні

В рамках подальшого розвитку співробітництва України з ЄС варто, перш за все, враховувати поточні тенденції співпраці між ЄС і США. Подальше співробітництво ЄС-США-Україна у сфері кібербезпеки доцільно зосередити на наступних напрямках [28; 29;30; 40]:

1 – завершити створення чіткої робочої системи координації у сфері кібербезпеки для повної імплементації Стратегії кібербезпеки України щоб залучити усіх національних акторів, включаючи неурядові організації, і зробити допомогу США, ЄС та інших організацій більш адресною та ефективною;

2 – використати досвід та практики ЄС і США для створення широкої національної схеми сертифікації з кібербезпеки, розробки плану, як відповідати на широкомасштабні інциденти і кризи, поглиблювати державно-приватне партнерство і посилювати дослідження;

3 – ініціювати приєднання України до Центру передового досвіду США з кібероборони, що допоможе Україні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері;

4 – нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду США з кібербезпеки та у співпраці з Румунією;

5 – розвинути співробітництво з посилення кібербезпеки в Україні для попередження і нейтралізації можливого російського втручання під час виборчих кампаній в Україні;

6 – продовжувати діяльність з визначення критичної інфраструктури та її ключових операційних вразливостей;

7 – опрацювати загальнонаціональний План реагування на надзвичайніситуації в кіберпросторі;

8 – розробити механізм розподілення ризиків через використання захищених хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади;

9 – залучити кращі західні практики задля посилення міжвідомчого співробітництва та державно-приватного партнерства з виробленням конкретного дієвого механізму його практичного застосування;

10 – пропонувати з боку США і ЄС та залучити з боку України більше зовнішньої експертної допомоги;

11 – спільними зусиллями розробити систему мотивації для фахівців, зайнятих у сфері кібербезпеки та кібероборони.

Також важливим напрямком співпраці може стати моніторинг російської та китайської кібер-активності, взаємодії кібер-організацій обох країн. В полі спільної уваги може бути вивчення можливостей рф використовувати лінії технологічного оптико-волоконного зв'язку безтранзитних газопровідних систем типу «Північний потік», «Північний потік-2», «Турецький потік» та їх продовжень по території країн НАТО та ЄС для вирішення непрофільних завдань, в тому числі, для кібершпигунства.

Цілі розвитку безпекового співробітництва ЄС і НАТО співпадають, і це базується не лише на тому факторі, що 22 країни є одночасно членами і ЄС, і НАТО, але й на бажанні взаємного заповнення поточних прогалин у безпекових можливостях один одного, зокрема у сфері кібербезпеки [31;32]. Для розвитку такої співпраці, а також взаємодії з іншими акторами, зокрема, Україною, був розроблений Рамковий документ з спільного дипломатичного реагування ЄС на шкідливу кібердіяльність (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities). Важливою віхою розвитку співпраці ЄС і НАТО з кібербезпеки стало встановлення Центром передового досвіду НАТО з кібероборони у 2013 році зв'язків з Європейським оборонним агентством для обміну інформацією, проведення спільних навчань і заходів та уникання дублювання досліджень у кіберсфері. Дві структури провели низку спільних навчань, зокрема – вже згадане навчання «Кібер Коаліція» (Cyber Coalition) і

навчання «Кібер Європа» (Cyber Europe), які стали платформою для спільних підходів. Нинішня актуалізація гібридних викликів і загроз, пов'язана з агресією Росії проти України, надає додаткового поштовху поглибленню взаємодії двох організацій. В лютому 2016 року, ще до схвалення Спільної заяви ЄС-НАТО, дві організації підписали Технічну угоду про співпрацю з кібероборони за напрямками обміну інформацією, тренування, досліджень і навчання. В результаті, практична співпраця розвивається між Групою реагування на комп'ютерні надзвичайні ситуації ЄС (CERT-EU) і Центром можливостей з реагування на комп'ютерні інциденти (NCIRC), які й стали підписантами згаданої технічної угоди від імені ЄС і НАТО.

На саміті НАТО 11-12 липня 2018 року у новій штаб-квартирі в Брюсселі розширене співробітництво між ЄС і НАТО відсвяткувало свій другий рік. Співпраця між ЄС і НАТО зросла в усіх сферах, від гібридних загроз та кібербезпеки до морського співробітництва.

Кібербезпека постійно присутня в їхніх офіційних документах. В рамках Розширеної співпраці між ЄС і НАТО із залученням третіх сторін, зокрема, з кібербезпеки, на даний час існують три пілотні країни: Молдова, Туніс та Боснія і Герцеговина. Третій звіт про хід її імплементації, схвалений Радами ЄС та НАТО,20 визначає, що обмін інформацією, включаючи й між-штабні політичні консультації, також матимуть місце й для України. Україна має багато кваліфікованих експертів у кіберсфері.

Проте, їм все ще не вистачає міжвідомчої координації та співпраці з міжнародними партнерами. Наприклад, Консультативна місія ЄС в Україні співпрацює з Кіберполіцією України, Службою безпеки України та Національним центром координації кібербезпеки при РНБОУ. Тим часом, належна координація залишається важливою проблемою, оскільки вона не залежить від стратегій чи політик, які вони розробляють.

Так само кошти та зусилля донорів залежать від рівня міжвідомчої координації в Україні. Україна співпрацює з ЄС і НАТО у сфері кібербезпеки поки що сепаратно, хоча в окремих випадках, переважно на рівні практичної

допомоги, дві організації здійснюють щонайменше узгодження своїх зусиль, адже ця двостороння допомога має бути скоординована у відповідності до засад співробітництва ЄС-НАТО у сфері кібербезпеки.

В Європейській службі зовнішньої дії вважають, що комплексний характер кіберпростору вимагає спільних зусиль урядів, приватного сектору, експертного середовища, технічної спільноти, користувачів і науковців з протидії сучасним кіберзагрозам. Як повідомив представник Підрозділу координації кіберполітики, попередження конфліктів і політики безпеки Європейської служби зовнішньої дії Елоїз Діволь на міжнародній конференції "Нові формати співпраці НАТО і ЄС з Україною" 30-31 травня 2018 року у Києві, ЄС звертає увагу на необхідність адаптації країн-партнерів, включаючи Україну, до правил кібербезпеки ЄС, пріоритетними серед яких є сертифікація програмного забезпечення, процес передачі звітності, впровадження норм відповідальності за дії в кіберпросторі.

Отже, можна констатувати, що ЄС нарощує свій потенціал у сфері тотальної діджіталізації, максимально намагаючись впроваджувати цифрові технології у всі сфери життєдіяльності європейського суспільства. Основним базовим документом в ЄС, який регулюватиме сферу кіберзахисту, є оновлена Стратегія кібербезпеки на 2021 – 2027 роки. ЄС концептуально має намір та вживає заходів з метою оперативного реагування на виклики та загрози сучасності в інформаційній сфері.

На прикладі США виявлено багато чинників, які сприяли проведенню успішної політики інформаційної безпеки. Серед них виділено нормативно-правове регулювання, вдалу політику державних органів та адміністрації президента, інформованість та довіру населення, кібер-страхування та міжнародну співпрацю.

Враховуючі політичні реалії та сучасні спрямування, Україна має активізувати співробітництво у сфері забезпечення кібербезпеки за такими напрямами: створення механізму оперативної координації та взаємодії, обміну інформацією про кіберзагрози й кіберінциденти між компетентними органами

України та ЄС; вдосконалення міжнародного співробітництва у сфері кібербезпеки; імплементація міжнародноправових та європейських норм у національне законодавство України, особливо щодо запровадження режиму кіберсанкцій [10; 37;38; 39; 40].

Між Україною та Сполученими Штатами Америки існує стратегічне партнерство, яке треба постійно розвивати. Першочерговим аспектом залишаються фінансова підтримка та технічна допомога для України з боку США. Аналіз викладених матеріалів дозволяє констатувати, що США й надалі готові відігравати важливу роль у забезпеченні кібербезпеки України.

Досвід США у цій площині переконливо демонструє, що в сучасному світі кіберпростір стає ареною як наступальних так і оборонних операцій, вимагає концентрації зусиль військового та цивільного секторів у фокусі цієї проблеми, що є наслідком чіткого визначення супротивників та союзників. Засади державної кібербезпекової політики США демонструють, що ця країна визначає кібербезпеку як важливу складову національної безпеки та докладає кардинальних зусиль з метою її посилення та забезпечення, у зв’язку з чим на законодавчому рівні схвалюються нормативні акти, які є своєрідною реакцією на поширення новітніх загроз у кіберпросторі [11].

# РОЗДІЛ 3
# РЕАЛІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

## 3.1. Удосконалення нормативно-правового забезпечення України у сфері інформаційної безпеки

Цифровий простір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою публічного управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету.

Однак кіберпростір надає нам не тільки ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики інформаційної бербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти.

В наші дні національна безпека неможлива без її кібербезпеки, а модернізація країни неможлива без її інформатизації. З огляду на вищенаведение варто визначитися з термінами. До сьогодні в публікаціях можна зустріти різні поняття, що використовуються як синоніми, зокрема, «безпека інформації», «інформаційна безпека», «кібербезпека» – автори, підміняючи між собою ці поняття вводять певну невизначеність.

Поняття «безпека інформації» визначено у ISO/IEC 27000 п. 3.28 (information security) «Безпека інформації» - збереження конфіденційності (3.10), цілісності (3.36) та доступності (3.7) інформації. Відповідно до Примітки 1 для кваліфікації безпеки в сфері інформації мають враховуватися і інші властивості, такі як справжність (3.6), звітність, неприйняття (3.48) та надійність (3.55) [1]. В національному вимірі поняття безпека інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних.

Вперше поняття «інформаційної безпеки» в Україні було визначено у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. № 537-V [2], в якому інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

– неповноту, невчасність та невірогідність інформації, що використовується;

– негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій;

– несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Згідно з Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

– створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

– вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Як бачимо, поняття «інформаційна безпека» набагато ширша ніж поняття безпеки інформації і зовсім не зводиться до неї.

Стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації у кіберпросторі. При цьому, кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [3]. Відповідно до ДСТ України ISO/IEC 27032:2016 п. 4.21 Кіберпростір – це складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення та послуг у мережі Інтернет, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь-якій фізичній формі.

Розвиток нового типу протистояння, як інформаційна боротьба, перехід гонки технічних озброєнь в кіберпростір також обумовлюють актуальність дослідження відносин держав в сфері кібербезпеки.

На думку фахівців збройних сил США в області кібербезпеки, станом на 2008 рік, в технічному плані повна адекватна система кіберзахисту передбачала побудову та використання таких основних підсистем:

– підсистеми захисту (Protection Capabilities), що забезпечує скритність випромінювань радіоелектронних засобів, систем і засобів зв'язку, комп'ютерну безпеку (Computer Security) і інформаційну безпеку (InfoSec);

– підсистеми виявлення (Detection Capabilities), що забезпечує розпізнавання аномалій в мережі за рахунок застосування систем їх виявлення;

– підсистеми реагування на зміни технічних параметрів і обстановки (Reaction Capabilities), що забезпечує відновлення (в тому числі реконфігурацію) і виконання інших процесів інформаційних операцій.

На думку окремих авторів, система кіберзахисту, створена відповідно до вищезазначених вимог, не забезпечує повною мірою кібербезпеки об'єкта інформатизації, і, в першу чергу, органів державної влади та оборони. Забезпечення кібербезпеки цих органів має здійснюватися єдиною інтелектуальною системою кібербезпеки, що є частиною системи інформаційної безпеки. При цьому в основу побудови перспективної системи

кібербезпеки має бути покладено поняття еволюції системи, тобто здатність її адаптації через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак) і технологій, що застосовуються для протидії їм протягом свого життєвого циклу [4].

Безумовно, створення такої системи можливо лише шляхом поєднання всього спектру заходів державного регулювання від законодавчого регулювання до ефективного та відповідального правозастосування, в основі яких буде лежати ризик-менеджмент.

В сучасних умовах структура кіберкомандування США охоплює понад 50 тис. осіб і представляє собою складну багаторівневу структуру, що об’єднує зусилля Міністерства оборони США, АНБ та Кіберкомандування США і нараховує 133 бойові команди чисельністю понад 6,2 тис. осіб.

Каталізатором законодавчих змін в сфері кібербезпеки в нашій державі стала гібридна війна, розв’язана рф із застосуванням як класичної, так і нелетальної зброї, в тому числі у кіберпросторі та через кіберпростір. 21-25 травня 2014 року відбулися DDoS-атаки і злом сайту ЦВК під час президентських виборів, внаслідок яких на сайті з'явилися помилкові результати. Незважаючи на повідомлення про злом, саме ці дані були озвучені в новинах на російському Першому каналі як реальні результати виборів в Україні, 23 грудня 2015 року за допомогою троянської програми BlackEnergy3, в використанні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго. Ці та багато інших, але не так широко відомих кібератак змусили серйозно задуматися і переглянути підходи до кібербезпеки не тільки лідируючі технологічні компанії, але і в цілому, винести це питання на державний рівень. Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року [5], а

реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [6].

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України», правову основу кібербезпеки України становили Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Забезпечення кібербезпеки в Україні ґрунтується на принципах:

– верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист

відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері інформаційної безпеки та ін.

Національна система кібербезпеки представляє собою комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України діяльність яких спрямована на забезпечення інформаційної безпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [33; 34; 35; 36; 38; 39; 40].

Результатом впровадження зазначених нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого має стати огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Важливим кроком на шляху створення сучасної системи кіберзахисту України стало прийняття Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [7], яким встановлено:

– визначення загальних вимог з кіберзахисту об’єктів критичної інфраструктури;

– встановлення обов’язкових заходів забезпечення захисту від кібератак;

– запобігання порушенню конфіденційності;

– цілісності та доступності інформаційних ресурсів;

– сталого функціонування.

Забезпечення безпеки в кіберпросторі не вичерпується заходами державного регулювання і контролю, а в багатьох випадках залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема, суб’єктів господарювання. Підвищений інтерес у кіберзлочинців викликає ринок криптовалют та електронної комерції. За допомогою різних способів здійснення атак, хакери здійснюють крадіжки електронних грошей безпосередньо у їх власників, або ж використовують для цього підручні ресурси - гаманці, біржі та інше. Кібератаки на суб’єктів господарювання та їх діяльність можуть набувати абсолютно різних форм. Це може бути фішинг, який здійснюється, наприклад, за допомогою розсилки електронних повідомлень співробітникам або використання шкідливого програмного забезпечення [35; 36].

Одним з ключових чинників, що сприяє попередженню кібератак є ефективна система захисту та жорстка система покарань кіберзлочинців, наприклад, така як існує у США. Україна, на жаль, на даний момент не може похвалитися настільки розвиненим і вдосконаленим законодавством щодо притягнення до відповідальності за незаконні шкідливі дії хакерів.

Окремо необхідно зауважити на те, що згідно із статтею 5 Закону (про основні засади) суб’єктами забезпечення кібербезпеки є і окремі громадяни які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. І тому саме від їх відповідальної поведінки у кіберпросторі найчастіше залежить стабільність кіберпростору [40].

Сьогодні законодавче регулювання кіберзахисту в Україні знаходиться на початку свого формування, проте, найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту пройдено. Безумовно, на цьому шляху ще багато проблем, але є і досягнення. Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури та інші, триває розробка підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання в сфері інформаційної безпеки.

Інформаційна війна, яка відбувається між росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібератак. З огляду на це формування нормативної основи забезпечення інформаційної безпеки має бути засноване на чіткій та зрозумілій Стратегії. Слід враховувати наявний досвід, як професійного середовища, так і іноземних партнерів у наступній Стратегії кібербезпеки України. Проте, це завдання є спільним як для держави, так і для суспільства в цілому, оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного.

Затвердження у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері.

За роки реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України", який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ,

організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту.

Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України.

Розбудовується Національна телекомунікаційна мережа, утворюється Національний центр резервування державних інформаційних ресурсів, забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України - Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері.

Активно розвивається співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Федеративною Республікою Німеччина, Королівством Нідерланди, Японією тощо), поглиблюється співробітництво з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій.

Започатковано проведення щорічного заходу - місяця кібербезпеки.

Водночас діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан

реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки.

## 3.2. Перспективні напрямки застосування заходів інформаційної безпеки в органах публічного управління

Важливим є дотримання ешелонованого захисту для більшого ефекту і кращого результату. Для захисту персональних комп'ютерів, ноутбуків, серверів, пропонується використовувати антивірус. Завдання антивірусу – боротися з типовими та масовими загрозами. Також пропонується звернути увагу на платформи, орієнтовані на виявлення цільових атак і складних загроз (Endpoint Detection and Response). При цьому EDR-рішення не можуть повністю замінити антивіруси, оскільки ці дві технології вирішують різні завдання [33; 34; 35; 36; 38; 39].

Для комплексного захисту мережі компанії, рекомендується використовувати міжмережевий екран наступного покоління (Next Generation Firewall). NGFW є своєрідним бар'єром між комп'ютерними мережами. Він як охоронець стежить за порядком в мережі підприємства, що охороняється, і фільтрує відвідувачів. Також може заборонити доступ до мережі деяким особистостям, яких вважатиме підозрілими.

Для запобігання фішингу потрібно використовувати платформи навчання кібербезпеці і підвищення обізнаності персоналу. Платформа використовує індивідуальний потрійний підхід: антифішингова оцінка, моніторинг та навчання. Система постійно розсилає співробітникам замасковані електронні листи з використанням різних імітацій сценаріїв атак. Реакція співробітників перевіряється різними методами і рівнями обману. Також платформа поєднує короткі навчальні модулі з вікториною для підвищення залученості співробітників.

При міграції в хмару слід звернути увагу на рішення Secure Access Service Edge – так звані служби безпечного доступу. Це комплекс рішень, який об'єднує хмарні служби безпеки мережі. SASE спрощує централізоване управління та знижує витрати на обслуговування, об'єднуючи всі компоненти в єдину платформу.

SASE надає змогу компаніям підключатися до єдиної, безпечної хмарної мережі як сервісу, при цьому мати доступ і до фізичних, і до хмарних ресурсів. Він підходить для захисту віддаленого робочого місця, підвищує мобільність користувачів, суттєво спрощує міграцію в «хмару».

Огляд загальної ситуації на 2024 рік: для запобігання фішингу потрібно використовувати платформи навчання кібербезпеці і підвищення обізнаності персоналу. Платформа використовує індивідуальний потрійний підхід: антифішингова оцінка, моніторинг та навчання. Система постійно розсилає співробітникам замасковані електронні листи з використанням різних імітацій сценаріїв атак. Реакція співробітників перевіряється різними методами і рівнями обману. Також платформа поєднує короткі навчальні модулі з вікториною для підвищення залученості співробітників [33; 34].

Перш ніж перейти до огляду інструментів, які допоможуть виявити наявні вразливості та посилити кібербезпеку, необхідно подивитися на загальну тенденцію хакерських атак.

Перший масштабний інцидент стався в ніч з 13 на 14 січня, коли від дій кіберзлочинців постраждало близько 70 сайтів урядових організацій. Продовж поточного року ми регулярно бачимо заяви Урядової команди реагування на комп’ютерні надзвичайні події України про активність хакерів. За даними CERT-UA у першому півріччі 2022 року було зафіксовано 1350 кібератак.

Проаналізувавши ці данні, можна побачити, що основною ціллю кіберзлочинців є сайти державних органів та органів місцевого самоврядування.

Стратегія безпеки: головною особливістю роботи українських органів управління та місцевого самоврядування можна вважати використання продуктів компанії Microsoft, таких як опараційні системи сімейства Windows, Microsoft 365, Dynamics 365 або сервіси Azure. Тому слід розглядати насамперед рішення для цієї групи продуктів.

В організації стратегії безпеки компанії будь-якого масштабу з будь-якої галузі, Microsoft рекомендує орієнтуватися на модель захисту Zero Trust на

Рис. 1. Вона адаптована до складного сучасного середовища й дозволяє захищати користувачів, пристрої, програми, дані та інфраструктуру.

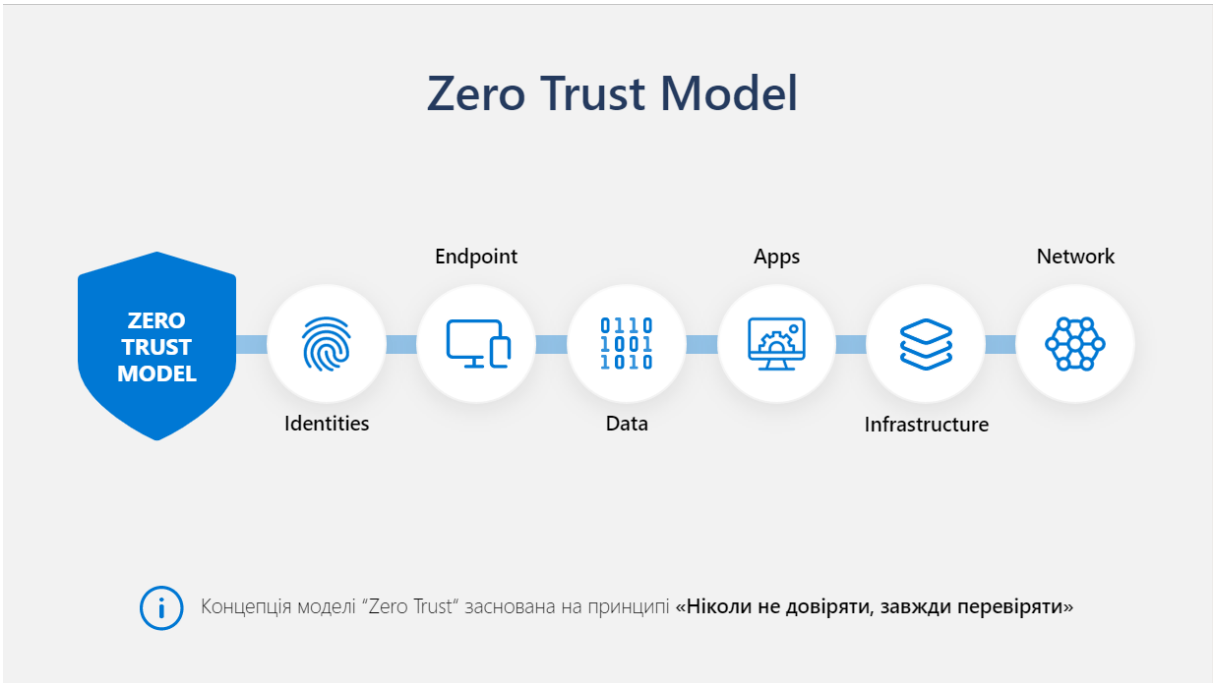


Рис. 1. Модель захисту Zero Trust

Модель Zero Trust працює за наступним принципом: чим більшу кількість сервісів ми налаштуємо для захисту інфраструктури компанії, тим більше сигналів про порушення безпеки зможемо отримати та швидко відреагувати на них.

Управління ідентифікацією та доступом: основою захисту за моделлю нульової довіри й першим, з чого розпочинаємо впровадження політик безпеки, є налаштування сервісів для ідентифікації.

В деяких компаніях співробітники продовжують використовувати Basic authentification, що передбачає використання ім’я користувача та пароля для запитів доступу. Такий спосіб аутентифікації більше не забезпечує захист конфіденційності облікових даних і залишає зловмисникам можливості для атак.

Саме тому базова ланка захисту в Identity – це налаштування Modern authentification, що передбачає використання сучасного метода аутентифікації – MFA(рис. 2). Це додає до процесу входу ще один рівень захисту.

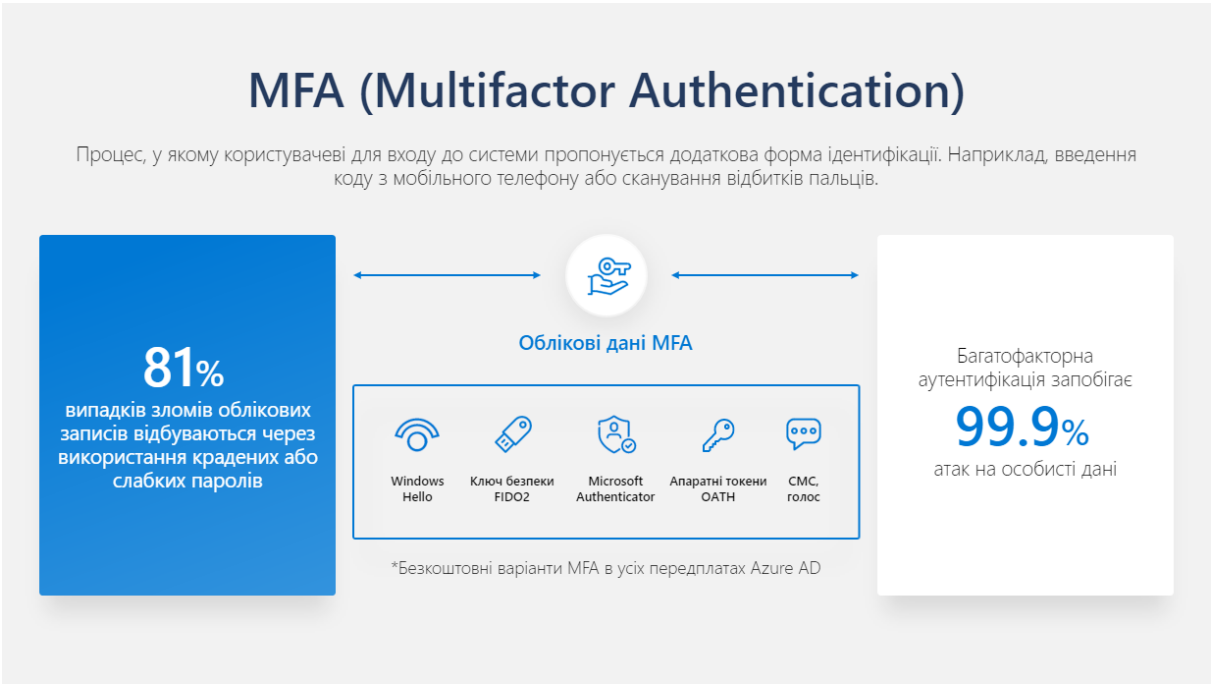


Рис. 2 Метод аутентифікації MFA

Таким чином завдяки MFA з’являється додатковий рівень захисту під час входу в облікові записи, що, за даними Microsoft, знижує ризики їх компрометації на 99,9%.

Також у ланці захисту Identities є ще одна вкрай важлива функція для управління доступом – Conditional-access (рис. 3).

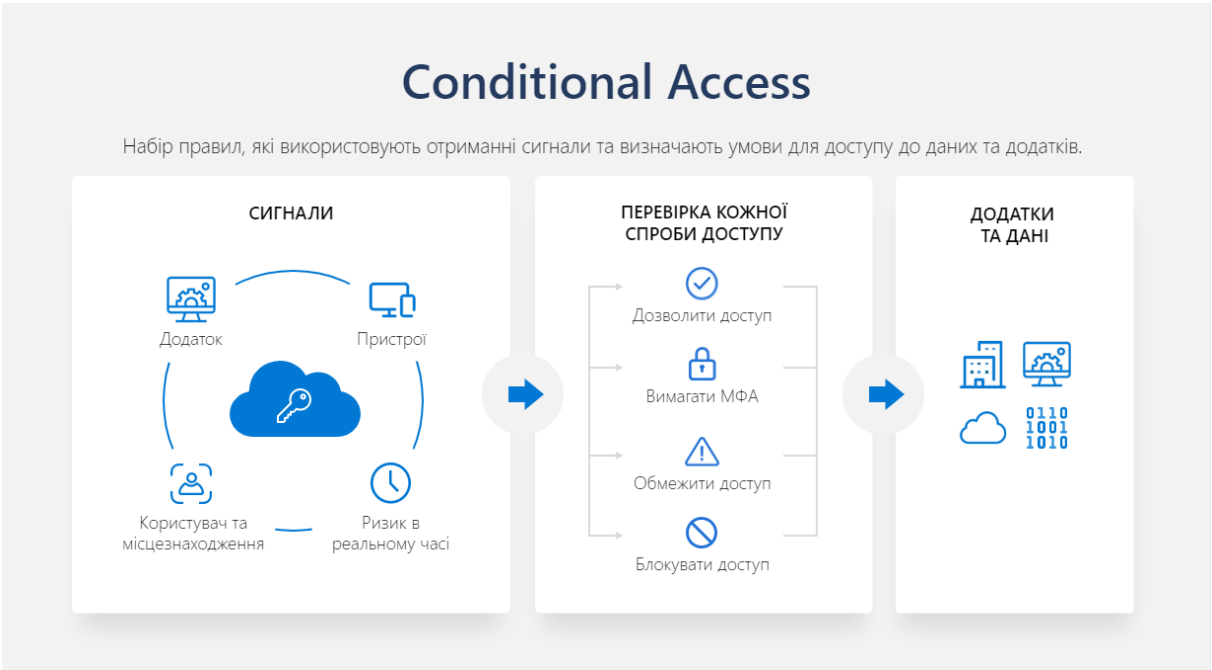


Рис. 3. Управління доступом Conditional-access

Це налаштування механізму перевірки кожного процесу підключення до корпоративної системи на основі створеного сценарію з можливостями заборонити доступ, дозволити без умов чи дозволити з умовами.

Захист кінцевих точок: у сучасних компаніях є великий вибір девайсів, які:

- управляються компанією,
- управляються співробітниками – BYOD,
- управляються сторонніми організаціями.

Це відкриває необмежені можливості для атак. Налаштування сервісів Endpoint Management, серед яких першочергово використовують Microsoft Intune(рис. 4), дає змогу управляти мобільними пристроями Intune (MDM) та управляти програмним забезпеченням Intune (MAM).

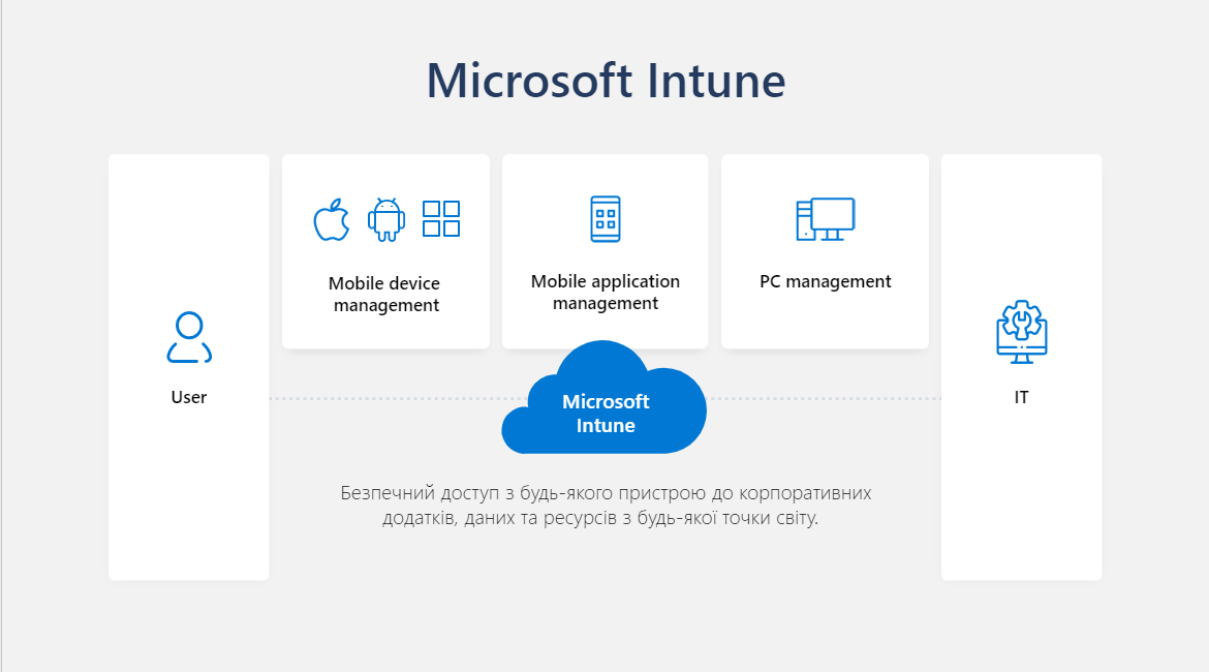


Рис. 4 Структура Microsoft Intune

Наприклад, коли користувач пройшов ідентифікацію у корпоративному обліковому записі та отримав доступ до документа з конфіденційною інформацією, необхідно запобігти збереженню цього документа в незахищеному місці або заборонити його спільне використання у месенджері, який не є корпоративним.

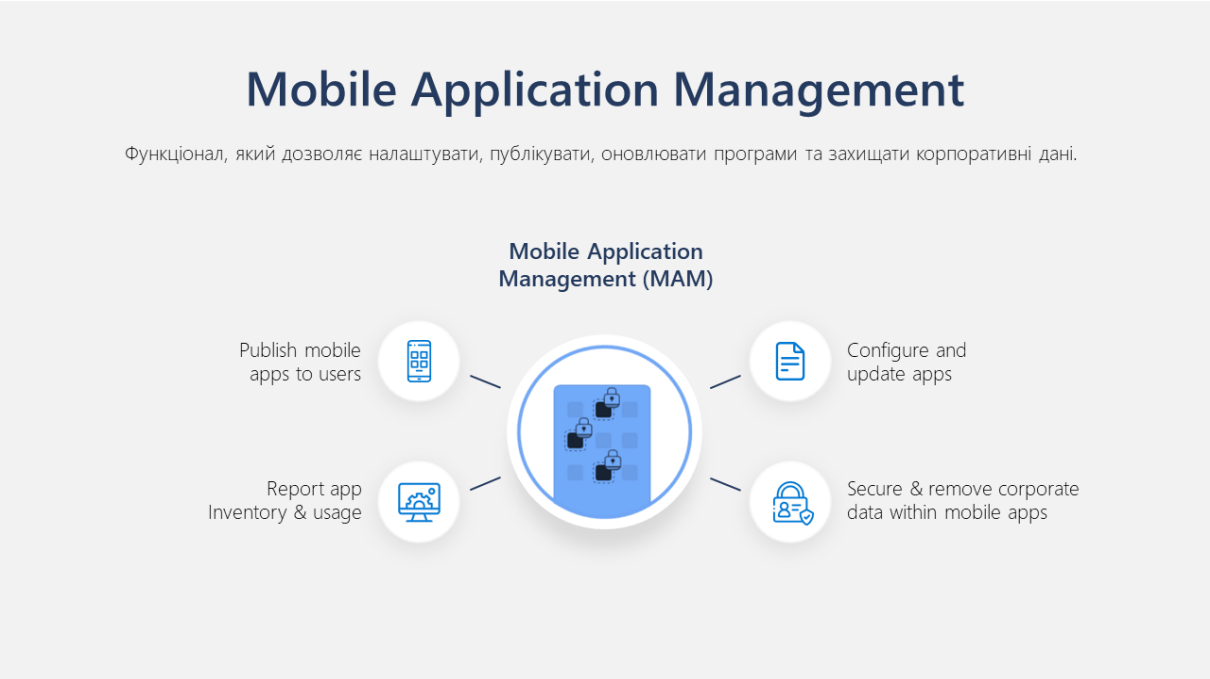


Рис. 5 Політики захисту Intune MAM

За наявності політик захисту Intune MAM (рис. 3.5), співробітники можуть передавати або копіювати дані тільки в довірених офісних програмах, таких як Word, Excel, Adobe Acrobat Reader, і зберігати їх тільки в надійних місцях, таких як OneDrive або SharePoint.

Intune MDM (рис. 6.) забезпечує централізоване керування кінцевими пристроями на платформах Android, iOS, Windows, MacOS.

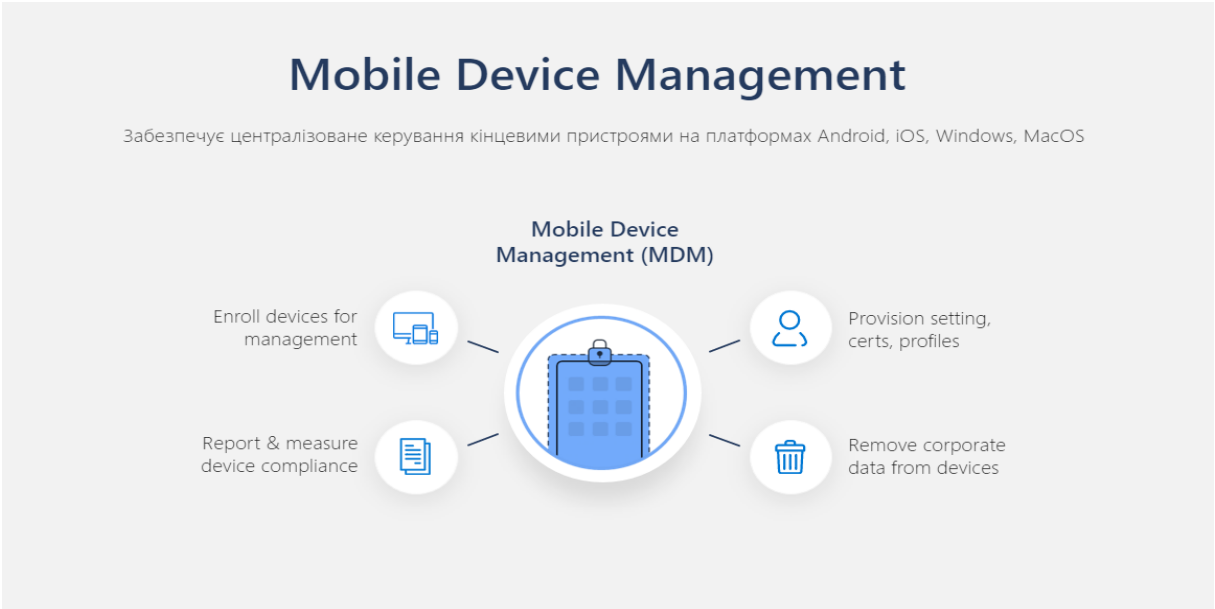


Рис. 6. Технології Intune MDM

Наприклад, при втраті пристрою або його крадіжці, можна віддалено видалити всі дані з нього. Працює це наступним чином: адміністратор через панель керування пристроями вибирає необхідний і запускає процес видалення. Якщо опцію «зберегти дані» не обрано, то всі дані облікового запису видаляються. Процес повторюється до успішного результату навіть після перезавантаження або відключення пристрою. І важливо те, що працює ця функція на Windows, Android, iOS, MacOS.

До речі, можливо також обмежувати встановлення додатків. Можна створити списки дозволених додатків в розділі Policy. Для цього необхідно лише додати посилання на додаток в магазині.

Для комплексного захисту кінцевих точок використовуємо сучасну платформу безпеки – Microsoft Defender for Endpoint.

Це рішення дає змогу швидко зупиняти атаки, масштабувати ресурси системи безпеки й удосконалювати захист для Windows, macOS, Linux, Android, iOS і мережевих пристроїв. Завдяки цьому можна контролювати свою інфраструктуру, протидіяти складним загрозам і реагувати на оповіщення з єдиної уніфікованої платформи, використовуючи інструменти та аналітику Microsoft Defender for Endpoint.

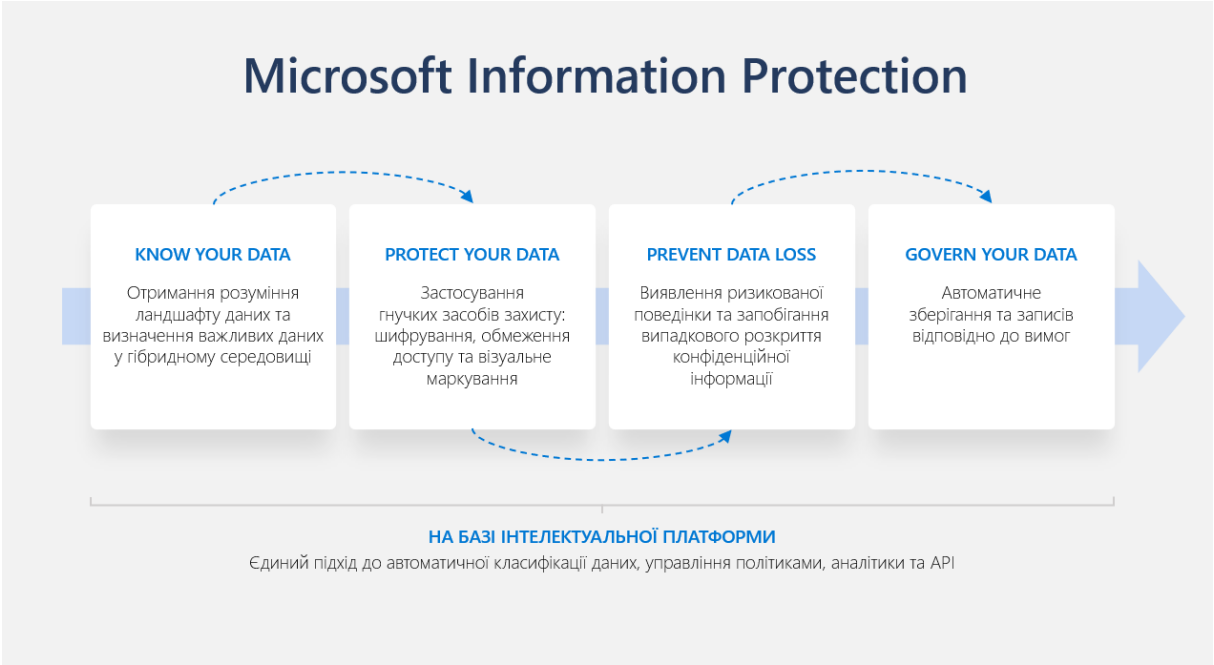


Рис. 7. Сервіси Microsoft Data Protection

Безпечна робота з корпоративними даними: у будь-якій компанії присутні об’єми даних, які необхідно захищати. Для цього у Microsoft є відповідні сервіси, які об’єднані у напрямок Data Protection (рис. 7).

Усю наявну в компанії інформацію треба спочатку класифікувати, щоб виявити надчутливі дані, визначити, де вони знаходяться, які групи користувачів мають до них доступ, та централізувати їх. Для застосування гнучких захисних дій, що включають шифрування, обмеження доступу та візуальне маркування використовується робота з мітками. Також необхідно визначити, яка інформація надається тільки для внутрішнього використання і є конфіденційною, та запобігти її випадковому поширенню за межами корпоративного середовища. Для цього треба використовувати можливості сервісу DLP (Data Loss Prevention).

Захист пошти: розглянемо комплексний підхід для захисту пошти з урахуванням найбільш поширених вразливостей. Якщо в компанії використовують пошту Exchange online, вона за замовчуванням включає хмарну службу Exchange online protection.

Це перша ланка фільтрації пошти, яка захищає вашу компанію від спаму, шкідливих програм та інших загроз електронної пошти. Але є ризик отримання листів зі шкідливими посиланнями або вкладеннями, тому можна рекомендувати організувати додатковий рівень захисту за допомогою Microsoft Defender for office 365. Для цього необхідно використовувати Microsoft Defender for office 365 Plan 1, яка включає розширені можливості запобігання загроз, наприклад, безпечні посилання – safe link, та безпечні вкладення – safe attach.

Safe link – функція, яка забезпечує сканування URL-адрес та допомагає захистити компанію від шкідливих посилань, що використовуються під час фішингу та інших атак.

Safe attach – функція, що забезпечує додатковий рівень захисту для вкладень електронної пошти перед їхньою доставкою одержувачам, а також

допомагає захистити організацію від непередбаченого обміну шкідливими файлами в SharePoint, OneDrive та Microsoft Teams.

Як співробітники будуть поводитись, якщо кіберзлочинці спробують дізнатися їх особисті дані або надішлють e-mail із запитом перейти за посиланням? Часто зловмисники діють через людей і використовують скомпрометовані адреси для розповсюдження шкідливого ПЗ.

Зі співробітниками треба проводити тренінги та виконувати симуляції фішингових атак, щоб подивитися на їхню поведінку. Можна найняти сторонню компанію для цього або зробити подібну симуляцію самостійно за допомогою Microsoft Defender for Office 365 – такий функціонал є у Plan2. Подібні тренінги підвищать рівень свідомості співробітників, їхньої підготовленості, здатності розпізнавати шкідливі повідомлення та не реагувати на них.

Виявлення потенційно небезпечних програм: щоб зрозуміти, які саме програмні комплекси використовують співробітники компанії й чи є вони надійними та безпечними, необхідно використовувати Microsoft Defender for Cloud Apps. Це рішення забезпечує повний контроль над конфіденційними даними завдяки всебічному моніторингу, аудиту та детальному контролю.

В Microsoft Defender for Cloud Apps є інструменти, які допомагають виявляти тіньові IT-ресурси (Shadow IT) (рис. 3.7) та оцінювати ризики, а також дозволяють застосовувати необхідні політики безпеки та проводити розслідування інцидентів.

Організація безпечної роботи в хмарі: інфраструктура компанії – це критичний вектор загроз. Microsoft Defender for Cloud – це платформа управління безпекою у хмарі та платформа захисту робочого навантаження у хмарі для ресурсів Azure.

Крім того, Microsoft Defender for Cloud (рис. 8) дає можливість захищати більшу кількість робочих процесів для таких хмарних платформ, як Amazon Web Services (AWS) та Google Cloud Platform (GCP).

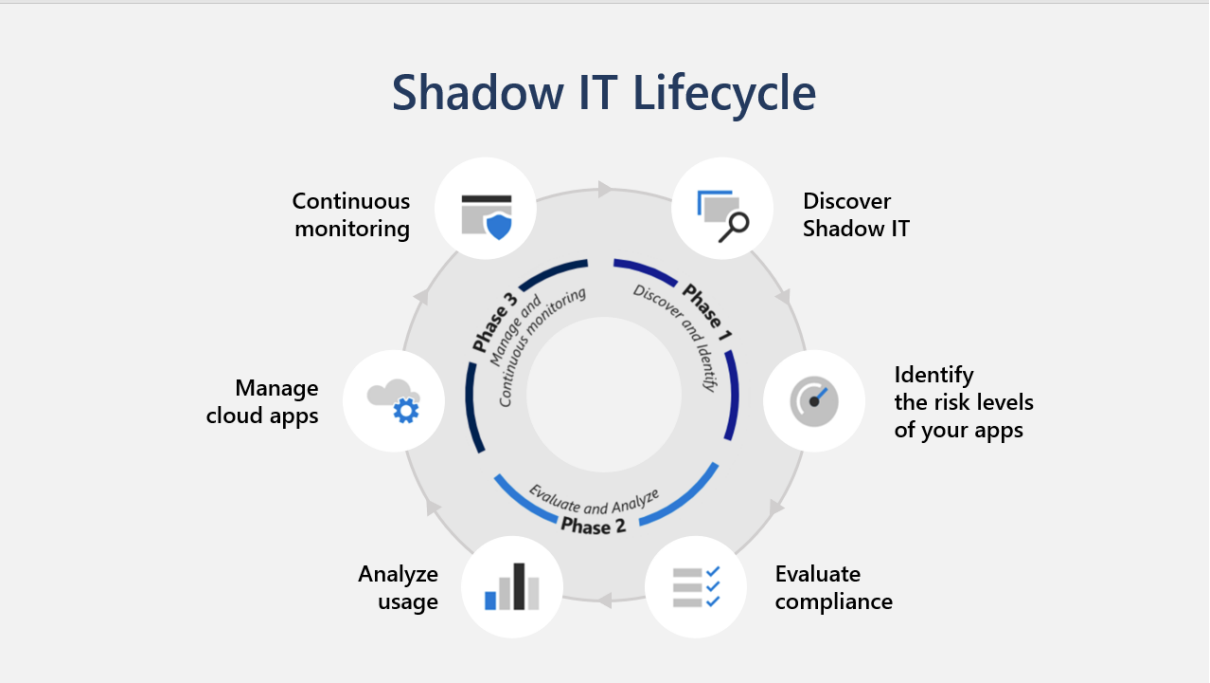


Рис. 8 IT-ресурси Shadow IT

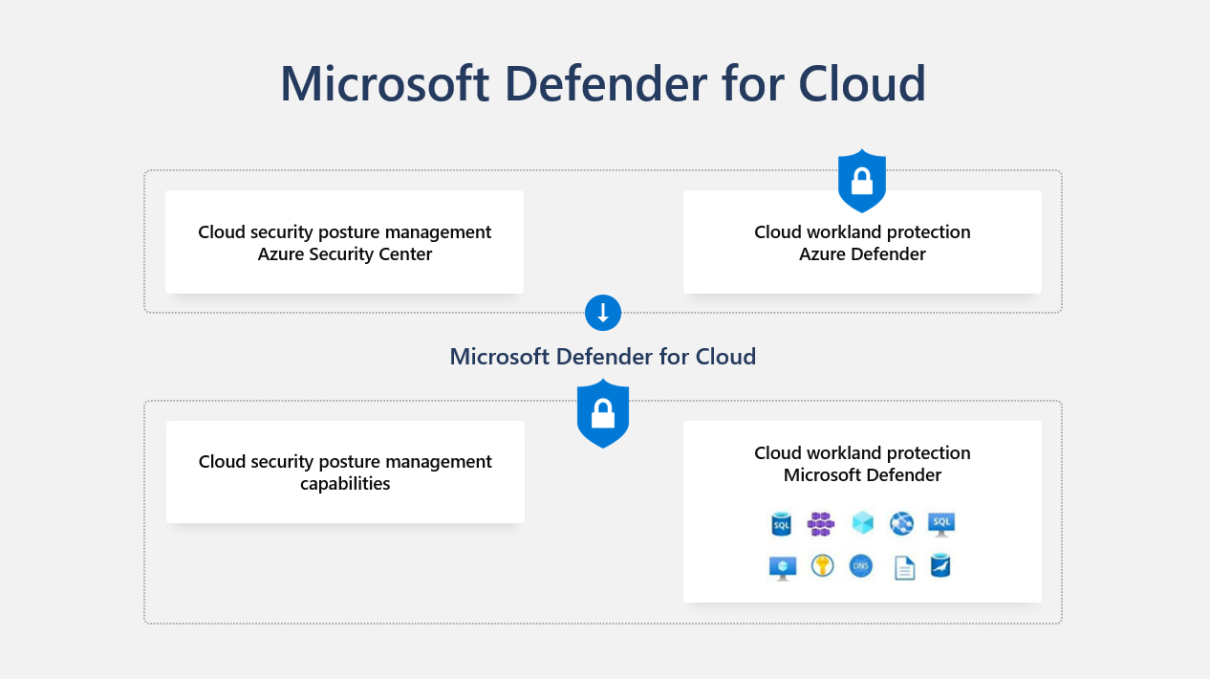


Рис. 9. Захист хмарних платформ Microsoft Defender for Cloud

Тобто у сучасної, прогресивної компанії, яка використовує хмарні технології по моделі multi-cloud, є можливість централізовано, з однієї консолі моніторити та налаштовувати політики безпеки.

Безпечний доступ до корпоративної мережі: безпека мережі вже давно не закінчується на обмеженні доступу ззовні. Треба шифрувати всі канали комунікації – зовнішні та внутрішні, обмежувати доступи за політиками, застосовувати мікросегментацію мереж та виявляти загрози в реальному часі.

Для цього у Microsoft розроблено цілий ряд продуктів, наприклад:

Azure Firewall – захист ресурсів віртуальної мережі Azure за допомогою орієнтованого на хмарне середовище брандмауера. Брандмауер Azure розгортається за хвилини, запобігає розповсюдженню шкідливих програм, забезпечує аналіз внутрішнього та зовнішнього трафіку в режимі реального часу та легко масштабується.

Захист від DDoS-атак – служба адаптивної аналітики загроз автоматично відстежує та усуває DDoS-атаки, функція усунення ризиків DDoS-атак очищає трафік на периметрі мережі до того, як трафік може вплинути на роботу додатків та служб.

Для забезпечення захисту мережі у Microsoft також є інші рішення, які слід впроваджувати під потреби конкретної компанії.

# ВИСНОВКИ

1. Досліджено сутність цифрової трансформації публічного управління. Наведено теоретичне узагальнення і нове вирішення наукової проблеми, яке виявляється у визначенні сутності цифрової трансформації публічного управління, особливостей забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування в Україні.

Аналіз керівних документів, наукових досліджень та сучасного стану забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування показав, що підвищення ефективності їх роботи можливе за рахунок удосконалення існуючих методів їх організації із застосування сучасних інформаційних технологій, своєчасного засвоєння нової нормативно-правової бази.

2. Обґрунтувано необхідність забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування. Завданням забезпечення кібербезпеки є створення необхідних умов у кіберпросторі, за яких можливим є досягнення загальнодержавних цілей та реалізація інтересів, завдань та цілей її елементів.

Вказано, що суб’єктами забезпечення кібернетичної безпеки інформаційних ресурсів є центральні органи виконавчої влади, органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових критичних об’єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист.

Основними об’єктами забезпечення кібербезпеки інформаційних ресурсів визначено національні цінності та національні інтереси як у кіберпросторі, так і в реальному просторі.

Для забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування насамеред повині буті розроблені процедури та план тестування та переконатися, що інші державні

органи дотримуються протоколу цифрової безпеки. Щоб бути захищеними від атак або загроз, органи управління, операцій, фінансів і зв'язку повинні пройти навчання щодо рекомендованих процесів і завдань для захисту даних держави.

3. Визначено досвід країн партнерів, що забезпечать швидкий, зручний та надійний спосіб забезпечення кібербезпеки інформаційних ресурсів між різнорівневими органами управління та самоврядування в Україні, щодо завдання кіберзахисту.

У сучасних умовах питання забезпечення кібербезпеки не обмежуються лише організацією системи захисту інформації на окремому об'єкті критичної інформаційної інфраструктури, а й передбачають створення єдиної системи захисту кібернетичного простору як складової частини інформаційної та національної безпеки будь-якої держави світу.

Нині більшість держав світу успішно проводять політику посилення кібербезпеки та її складників. У міжнародному форматі можна виділити три основні моделі правового врегулювання поширення інформації:

– перша модель передбачає тотальний, жорсткий контроль держави над мережею Інтернет;

– друга модель передбачає відповідальність провайдера за будь-які дії користувача;

– третя модель регулювання безпеки в мережі Інтернет передбачає звільнення провайдера від відповідальності в тому разі, якщо він виконує певні умови, пов'язані з характером надання послуг і взаємодії із суб'єктами інформаційного обміну.

4. Досліджено напрями забезпечення кібербезпеки у Європі, США та України. Враховуючі політичні реалії та сучасні спрямування, Україна має активізувати співробітництво у сфері забезпечення кібербезпеки за такими напрямами:

– створення механізму оперативної координації та взаємодії, обміну інформацією про кіберзагрози й кіберінциденти між компетентними органами України та з іншого боку ЄС та США;

– вдосконалення міжнародного співробітництва у сфері кібербезпеки;

– імплементація міжнародно-правових та європейських норм у національне законодавство України, особливо щодо запровадження режиму кіберсанкцій.

Аналіз викладених матеріалів дозволяє констатувати, що США й надалі готові відігравати важливу роль у забезпеченні кібербезпеки України. Засади державної кібербезпекової політики США демонструють, що ця країна визначає кібербезпеку як важливу складову національної безпеки та докладає кардинальних зусиль з метою її посилення та забезпечення, у зв’язку з чим на законодавчому рівні схвалюються нормативні акти, які є своєрідною реакцією на поширення новітніх загроз у кіберпросторі

5. Визначено можливості удосконалення нормативно-правової складової у сфері кібербезпеки інформаційних ресурсів. Результатом удосконалення існуючих нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого повинен бути огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена діючим законодавством.

Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об’єктів критичної інфраструктури та інші, триває розробка підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання в сфері кібербезпеки.

6. Розроблено пропозиції та перспективи подальших напрямів у сфері кібербезпеки.

Важливе значення для розвитку забезпечення кібербезпеки інформаційних ресурсів органів публічного управління має удосконалення методів та засобів підготовки фахівців, впровадження сучасних технологій. Враховуючи, що забезпечення кібербезпеки в інформаційних ресурсах постійно зростає, зростають й вимоги до підготовки керівних кадрів.

Для підвищення ефективності навчання державних фахівців необхідно систематично удосконалювати методи та засоби формування вмінь і навиків кібернетичної безпеки інформаційних ресурсів. Тому, для прискорення вирішення завдань кіберзахисту, інформаційні ресурси органів публічного управління та місцевого самоврядування повинні мати ефективні та зручні у використанні програмні засоби, що постійно розвиваються та оновлюються.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк В. В. Взаємодія державних та недержавних суб'єктів забезпечення інформаційної безпеки в процесі протидії збройній агресії РФ України. Вісн. Київ. Нац. ун-ту ім. Тараса Шевченко. Серія: Державне управління. 2016. № 3(17). С. 5–8.

2. Вербицький О. В. Поняття соціальної напруженості та роль держави в управлінні нею й інформаційною безпекою. Проблеми управління соціальним і гуманітарним розвитком: матеріали наук.- прак.конф. (01.12.2017 р.). Дніпро, 2017. С. 47–49.

3. Глобальні інформаційні ресурси як складова інформаційного забезпечення соціокультурної сфери сучасної України. *Тенденції впливу глобального інформаційного середовища на соціокультурну сферу України* / О. С. Онищенко, В. М. Горовий, В. І. Попик [та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ, 2013. С. 31–97.

4. Горова С. В. Особа в інформаційному суспільств і: виклики сьогодення : монографія; НАН України, Нац. б-ка України ім. В. І. Вернадського. К., 2017. 452 с.

5. Гуровський В. О. Роль органів державної влади у сфері забезпечення інформаційної безпеки України. Вісник Української академії державного управління при Президентові України. Київ, 2014. № 3.С. 21–31.

6. Гуцалюк М. Інформаційна безпека в сучасному суспільстві . *Право України*. 2005. № 7. С. 71–74.

7. Дацюк С. Проблеми інформаційної безпеки, які ігноруються *UAINFO*. 2017. 28.02. URL: http://uainfo.org/blognews/1488267836-problemi-informatsiynoyi-bezpeki-yaki-ignoruyutsya.html.

8. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти : монографія; НАПрН, НДНП НАН України, Нац. б-ка України ім. В. І Вернадського. Київ, 2015. 388 с.

9. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України:

онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–103.

10. Доктрина інформаційної безпеки України : Указ Президента України від 25 лютого 2017 р. № 47 URL: http://www.president.gov.ua/documents/472017-21374

11. Домбровська С. М. Механізми інформаційної безпеки як складові державної безпеки України. Державне управління науково-освітнього забезпечення підготовки конкурентоспроможних фахівців у сфері цивільного захисту: матеріали Всеукраїнської наук.-практ. конф. / за заг. ред. В. П. Садкового. Харків, 2015. С. 282–286.

12. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою. Радіоелектроніка, інформатика, управління. 2017. № 1. С. 107–114.

13. Єврокомісія визначила стратегічні цілі цифрового розвитку ЄС до 2030 року. URL: https://www.ukrinform.ua/rubric-world/3205020-evrokomisia-viznacila-strategicni-cili-cifrovogo-roz vitku-es-do-2030-roku.html

14. Європейське агентство з мережевої інформаційної безпеки (ENISA), 201 – Режим доступу: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss

15. Закон України про національну безпеку України URL: http://zakon0.rada.gov.ua/laws/show/2469-19/page

16. Зандстра М. PHP. Об'єкти, шаблони і методики програмування / М. Зандстра; [переклад з англ.: Тригуб С.]. - М.: Вільямс, 2011. - 560 с.

17. Кільченко А. В. Базові поняття і терміни веб-технологій [Електронний ресурс] / [А. В. Кільченко, О. І. Поповський, О-р. В. Тебенко, О- й. В.Тебенко, Н. М. Матросова]; Упорядник: Кільченко А. В. – Київ: ІІТЗН НАПН України, 2014. – 49 с. – Режим доступу: http://lib.iitta.gov.ua/6472/1/базові_поняття.pdf (дата звернення 18.04.2020 р.).

18. Комп’ютерна злочинність і інформаційна безпека / А. П. Леонов ; за заг. ред. А. П. Леонова. Мінськ : АРІЛ, 2000. 552 с.

19. Коржинський С. Н. Настільна книга Web-майстра: ефективне застосування HTML, CSS і JavaScript / С. Н. Коржинський - М.: КноРус, 2011. – 416 с.

20. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса: Юридична література, 2003. 314 с.

21. Крейн Д. AJAX в дії / Д. Крейн, Э. Паскарелло, Д. Джеймс. - М.: Вільямс, 2006. – 640 с.

22. Лужецький В. А., . Войнович О.П., Дудатьєв А. В. Інформаційна безпека : навч. посіб. Вінниця : УНІВЕРСУМ-Вінниця, 2009. 240 с.

23. Марков В.В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації . *Право і безпека*. 2013. № 1 (48). С. 78-80.

24. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: ХНЕУ, 2013. – 476 с.

25. Офіційний сайт jQuery [Електронний ресурс]. – Режим доступу: https://jquery.com / – (дата звернення 18.04.2020 р.)

26. Петрик В. М. Інформаційна безпека: соціально-правові аспекти: Підручник . К. : КНТ, 2010. 776 с.

27. Почепцов Г. Логика пропаганды, или Новости без грима / Г. Почепцов. – Режим доступа : http://osvita.mediasapiens.ua/trends/1411978127/logika_ propagandy_ili_novosti_bez_grima/.

28. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. А. Чукут. – К. : Знання, 2006. – 663 с.

29. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України. Розпорядження КМУвід 19 грудня 2023 р. №1163-р

30. Про основні засади забезпечення кібербезпеки України. Закон України 5 жовтня 2017 року № 2163-VIII - URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

31. Про рішення Ради національної безпеки і оборони України від 14

травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України від 26 серпня 2021 року № 447/2021

32. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" Указ Президента України від 15 березня 2016 року - URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

33. Реферат на тему: «Засоби створення Web-додатків» [Електронний ресурс]. – Точка доступу: URL: http://ifreestore.net/2267/ – Реферат на тему: «Засоби створення Web-додатків». (дата звернення 18.01.2020 р.).

34. Руководство по PHP [Електронний ресурс]. — Режим доступу: http://php.net/manual/en/intro-whatcando.php (дата звернення 17.04.2020р.)

35. Слинкин А. MySQL. Оптимізація продуктивності / А. Слинкин. - СПб.: Символ-Плюс, 2011. - 832 с.

36. Сучасні методи веб-програмування [Електронний ресурс] – Режим доступу до ресурсу: http://sites.znu.edu.ua/webprog/lect/1222.ukr.html. (дата звернення 18.04.2020 р.).

37. Тихомиров О.О. Класифікації забезпечення інформаційної безпеки URL: http://www.law.journalsofznu.zp.ua/archive/visnik-1-2011/29.pdf.

38. Ткачук Н.В. Стан та проблемні питання реалізації Стратегії кібербезпеки України. Інформація і право. № 1(28)/2019. С. 129-134.

39. Тузовский А. Ф. Проектування і розробка web-додатків: навч. посібник для академічного бакалаврату [Електронний ресурс] / А. Ф. Тузовский. - М.: Юрайт, 2017. – 218 с. - Режим доступу: https://stud.com.ua/97571/informatika/proektuvannya_i_rozrobka_web-dodatkiv (дата звернення 18.04.2020 р.). – Назва з екрана.Веб застосунок [Електронний ресурс]. – Точка доступу: URL: http://uk.wikipedia.org/wiki/Веб-застосунок– Веб застосунок. (дата звернення 18.04.2020 р.).

40. Формування стратегічного наративу інформаційного забезпечення реінтеграції тимчасово окупованих територій у загальноукраїнський контекст :

[монографія] / [В. Горовий (кер. проек ту), О.Онищенко, Ю.Половинчак та ін.] ; НАН України, Нац.б-ка України ім. В. І. Вернадського. Київ, 2017. 212 с.

41. Фримен А. jQuery 2.0 для професіоналів / А. Фримен. – М.: Вільямс, 2014. – 1040 с.

42. Чорна А. В. Можливості використання комп'ютерних засобів управління процесом розробки програмного забезпечення при вивченні дисциплін «Операційні системи і системне програмування» [Електронний ресурс] / А. В. Чорна // «Проблеми інженерно-педагогічної освіти», 2015, № 48-49. - Режим доступу: http://repo.uipa.edu.ua/jspui/bitstream/123456789/5440/1/30.pdf

43. Шатун В.Т. Інформаційна безпека – невід'ємна складова національної безпеки України . *Наукові праці. Державне управління*.2016. Вип. 255. Т. 267. С.174-180

44. Black C. Building a Single Page Web Application with Knockout / C. Black, D. Ly - Packt Publishing, 2014. – 152 с.

45. Bootstrap. – Режим доступу: http://getbootstrap.com/getting-started

46. Brendan Burns - Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. O'Reilly Media; 1ie ed. 2018. - 166 pages

47. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques. [Електронний ресурс] - Режим доступу: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/

48. Cyber Security Strategy Documents. URL: https://ccdcoe.org/strategies-policies.html;

49. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. – Режим доступу: https://ec.europa.eu/digital-singlemarket/ en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity.

50. *A European Agenda On Security*. (2017). Retrieved from https://home-affairs.ec.europa.eu/system/files/202009/20170907_a_european_agenda_on_security

_-_state_of_play_en.pdf

51. Europe's Digital Decade: Digitally empowered Europe by 2030. URL: https://ec.europa.eu/

52. Federal Government Cybersecurity Incident and Vulnerability Response Playbooks URL: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

53. ISO/IEC 15408-1999 «Common Criteria for Information Technology Security Evaluation».

54. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management».

55. ISO/IEC 25010:2011 [Електронний ресурс] .– Режим доступу URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en (дата звернення 15.05.2020 р.).

56. ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements».

57. Monteiro F. Learning Single-page Web Application Developmen / F. Monteiro - Packt Publishing, 2014. – 214 c.

58. ND TZI 2.5-004-99 "Criteria for evaluating the security of information in computer systems against unauthorized access".

59. Patrik Uytterhoeven, Rihards Olups Zabbix 4 Network Monitoring: Monitor the performance of your network devices and applications using the all-new Zabbix 4.0, 3rd Edition .–Packt Publishing Ltd, 21 січ. 2019 р. –: 798С.

60. Remarks by (he President on securing our nation’s cyber infrastructure). White House. URL: whitehouse.gov/ihe_press_ofIicc/Remarks-by-the-Presidcni-on-Sceuriiy-Nations-Cyber-Infrusimcture

61. ROADMAP: Proposal on a European Strategy for Internet Security http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

62. Sam Hampton-Smith Pro CSS3 Layout Techniques [Електронний ресурс]. Режим доступу: https://nildawangdye.files.wordpress.com/2017/05/pro-css3-layout-techniques-by-sam-hampton-smith.pdf (дата звернення 18.04.2020 р.)

63. The Administration’s Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure;

64. The benefits of Cyber Insurance. URL: https://www.loricainsurance.com/legacy/documents/Summary - Cyber.pdf.

65. The Department of Defense Cyber Strategy. URL: strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf;

66. US-CERT: Understanding Hidden Threats: Rootkits and Botnets. URL: https://www.us-cert.gov/ncas/tips.

67. What is cyber insurance and why you need it. URL: https://www.cio.com/article/3065655/cyber-attacksespionage/what-is-cyber-insurance-and-why-you-need-it.html