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

студента *Бєлозьорова Максима Анатолійовича*

академічної групи *281м-21з-2 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

на тему: *«Забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування»*

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

Рецензент:				

Нормоконтролер:	Вишневська О.В.			

Дніпро
2022

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему «Забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування».

72 стор., 11 рис., 50 джерел.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, КІБЕРБЕЗПЕКА, КІБЕРЗЛОЧИННІСТЬ, КІБЕРШПИГУНСТВО, КІБЕРТЕРОРИЗМ, ПУБЛІЧНЕ УПРАВЛІННЯ, МІСЦЕВЕ САМОВРЯДУВАННЯ, ІНФОРМАЦІЙНІ РЕСУРСИ.

Об’єкт дослідження це процес організації забезпечення кібербезпеки інформаційних ресурсів та сфери їх застосування в органах публічного управління та місцевого самоврядування.

Предмет дослідження – забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування.

Мета дослідження полягає у виявлення та обґрунтування потенційних можливостей у забезпеченні кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування, а саме часткова автоматизація, створення пропозицій та перспективи виконання завдання кіберзахисту в даних органах.

У першому розділі досліджуються теоретичні основи кібернетичної безпеки в публічному управлінні.

Другий розділ присвячено аналізу проблем у світовому досвіду забезпечення кібернетичної безпеки органів державного управління.

У третьому розділі реалізовано основні напрями забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування.

Сфера практичного застосування результатів роботи – інформаційні ресурси органів державного управління.

ABSTRACT

Explanatory note of the master's degree qualification thesis on the topic «Ensuring cyber security of information resources of public administration and local self-government bodies»

72 pages, 11 figures, 50 sources.

ENSURING CYBER SECURITY, CYBER SECURITY, CYBER CRIME, CYBER ESPIONAGE, CYBER TERRORISM, PUBLIC ADMINISTRATION, LOCAL GOVERNMENT, INFORMATION RESOURCES.

The object of the research is the process of organizing the cyber security of information resources and their scope of application in public administration and local self-government bodies.

The subject of the study is ensuring cyber security of information resources of public administration and local self-government bodies.

The purpose of the study is to identify and substantiate potential opportunities in ensuring the cyber security of information resources of public administration and local self-government bodies, namely partial automation, creation of proposals and prospects for the implementation of cyber protection tasks in these bodies.

The first chapter examines the theoretical foundations of cyber security in public administration.

The second chapter is devoted to the analysis of problems in the global experience of ensuring cyber security of state administration bodies.

In the third section, the main areas of ensuring cyber security of information resources of public administration and local self-government bodies are implemented.

The field of practical application of work results is the information resources of state administration bodies.

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) – складається 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 публічного 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[35] є мережа, створена на базі наявних і перспективних мереж зв'язку і передачі даних із застосуванням сучасних технологій.

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 [34] 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.

Мета роботи: виявлення та обґрунтування потенційних можливостей у забезпеченні кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування, а саме часткова автоматизація, створення пропозицій та перспективи виконання завдання кіберзахисту в даних органах.

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

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

– провести аналіз цифрової трансформації публічного управління в умовах кібернетичного захисту інформаційних ресурсів державних органів;

– провести аналіз концепцій цифрової безпеки у сучасному світі з розтлумаченням основних можливих загроз кібернетичного простору державного сектору управління;

– визначити основні напрямки забезпечення цифрової безпеки та постановки завдання на основі проведеного аналізу кібернетичної безпеки в публічному управління;

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

– провести формальний аналіз забезпечення кібернетичної безпеки у Європі, США та Україні в умовах кібернетичного захисту інформаційних ресурсів в органах державного управління;

– дослідити та проаналізувати нормативно-правову складову в сучасних умовах;

– визначити перспективи та пропозиції у сфері кібернетичного захисту інформаційних ресурсів органів державного управління;

– запропонувати можливі технічні рішення у даній сфері для зменшення витрат часу на виконання поставлених завдань;

– визначити подальші напрямки роботи.

Об’єкт дослідження: процес організації забезпечення кібербезпеки інформаційних ресурсів та сфери їх застосування в органах публічного управління та місцевого самоврядування.

Предмет дослідження: забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування.

В магістерській роботі були використані загальнонаукові теоретичні методи за допомогою яких були виконані завдання і досягнуто мету дослідження. Методологічною основою дослідження став структурно-функціональний метод, який використовувався для вирішення основних завдань роботи. Історичний та порівняльний методи дали змогу дослідити сучасний стан кібернетичного захисту інформаційних ресурсів країн партнерів, проаналізувати досвід роботи у цих галузях, як ЄС так і США у контексті євроатлантичної інтеграції України. За допомогою методів систематизації та узагальнення розглянуто інституційно-правові засади кібернетичного захисту в Україні на умовах війни. Методи аналізу, синтезу, індукції, дедукції, аналогії дали змогу проаналізувати сучасний стан державної політики України в секторі кіберзахисту інформаційних ресурсів державних органів управління у зв’язку з російською агресією. Для розроблення теоретичних рекомендацій дослідження та формулювання висновків роботи були використані методи прогнозування, аналізу і синтезу.

Інформаційною базою дослідження є законодавчі та нормативні акти України, наукові праці вітчизняних і закордонних учених, аналітичні матеріали міжнародних організацій, дані інформаційно-аналітичних бюлетенів і оглядів, наукові статті у фахових наукових виданнях, матеріали доповідей на наукових та науково-практичних конференціях, відкриті інформаційні ресурси мережі Інтернет, довідкова література.

РОЗДІЛ 1
АНАЛІЗ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ПУБЛІЧНОМУ УПРАВЛІННІ

Запропоновано виокремити загрози системі управління даних органів в окрему категорію для забезпечення можливості їх подальшого аналізу, прогнозування, і вироблення політики протидії.

Введена в дію указом Президента України №447/2021 від 14 травня 2021 року "Про Стратегію кібербезпеки України" [29] 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 кібербезпеки 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.

Насамперед розтлумачимо загальні поняття у забезпеченні кібернетичної безпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування таких[18], 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 [4].

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[38]. 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[6]. Це доступні для використання відомості в усіх сферах життєдіяльності людини, суспільства і держави, які зберігаються на відповідних носіях як документи[23], 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 політики, 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[26]. Як висновок це організуючий і регулюючий вплив держави суспільну життєдіяльність людей з метою її впорядкування, збереження чи перетворення, опираючись на владну силу, яку обмежує дієвий суспільний контроль.

Місцеве самоврядування – це право та змога територіальних громад як безпосередньо, так і через представницькі органи місцевого самоврядування в межах закону здійснювати регулювання й управління суттєвою часткою суспільних справ, які належать до їхньої компетенції, в інтересах місцевого населення. Органи місцевого самоврядування відповідають за шкільну і дошкільну освіту, охорону здоров'я первинного рівня (поліклініки, фапи),

заклади культури, благоустрій – освітлення вулиць, стан доріг, прибирання, громадський порядок і багато інших, важливих повсякденних питань.

Для протидії загрозам системі державного управління і міні-мізації 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.

1.1 Цифрова трансформація публічного управління

Інформаційні 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 [7].

Важливу роль в розвитку держави відіграє цифрова трансформація державного управління, головним фактором якої є інформація та знання, шляхи доступу до них. В сучасних умовах цифрова трансформація державного 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.

Цифровізація є ключовим фактором здорового розвитку 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. В державному секторі України «цифрові» технології – це один із основних напрямків реформування державного управління та конкретний приклад для всієї країни, яким чином потрібно використовувати переваги «цифрового» світу. Синергетичний потенціал мобільних, соціальних, «хмарних» технологій, «інтернету речей» та технологій аналізу даних сукупно здатні привести до істотних змін у державному управлінні та зробити державний сектор України реактивним, ефективним і ціннісним. Україна наразі вже має позитивні приклади використання «цифрових» технологій, наприклад, у сфері державних закупівель. В умовах становлення «цифрових» економік, коли громадяни стають фактично користувачами технологій, державні установи повинні робити стратегічні інвестиції в інформаційно-комунікаційні технології. Інакше вони виявляться не готовими до нових моделей взаємодії та обслуговування, стануть заручниками старих, нестійких моделей управління.

«Цифровізацію» необхідно розглядати як інструмент, а не як самоціль. При системному державному підході «цифрові» технології будуть стимулювати розвиток відкритого інформаційного суспільства як одного з істотних чинників розвитку в Україні демократії, економічного зростання, створення робочих місць, підвищення продуктивності, а також підвищення якості життя громадян України. Останнім часом в Україні було розроблено біля десятка законопроектів, які тією чи іншою мірою стосуються сфери «цифровізації» та інформаційно-комунікаційних технологій, а деякі з них вже стали законами України.

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 полегшують 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.

Головними проблеми, які потрібно усунути, щоб процес цифровізації розвивався і досяг своєї мети, є: зростання кіберзлочинності в умовах збільшення кількості інформаційних систем, які використовують персональні дані[25]; відсутність захищеного обміну ідентифікаційними даними фізичних та юридичних осіб, які обробляються в інформаційних системах державних органів і приватного сектору, відсутність підтвердження ідентифікаційних даних; використання в системах реєстрації та контролю доступу до інформаційних систем технологічно несумісних механізмів, алгоритмів і протоколів електронної ідентифікації та впізнання.

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.

1.2 Концепції цифрової безпеки

Кіберзахист інформаційних ресурсів сьогодні є об’єктивним процесом, що заповнює всі сфери соціального існування, у тому числі діяльності в секторі публічного управління та місцевого самоврядування. Нове інформаційне середовище дозволить не тільки накопичувати необхідні дані про життя і події в суспільстві й за кордоном у базах даних і знань, в експертних системах[32], 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.

Три основні концепції безпеки, важливі для інформації в Інтернеті: конфіденційність, цілісність і доступність. Концепції, що стосуються людей, які використовують цю інформацію автентифікація, авторизація та неспростовність.

Коли інформація читається або копіюється кимось, не уповноваженим на це, результат є відомий як втрата конфіденційності. Для деяких видів інформації конфіденційність є дуже важливою важливий атрибут. Приклади включають дані досліджень, медичні та страхові документи, нові специфікації продукції та державні інвестиційні стратегії. У деяких місцях може бути бути юридичним зобов’язанням щодо захисту приватного життя осіб. Це особливо вірно для органів публічного управління та державного банку; підприємств, які надають кредит своїм клієнтів або видавати кредитні картки; лікарні, кабінети лікарів і медичне обстеження лабораторії; особи або агентства, які пропонують такі

послуги, як психологічне консультування або медикаментозне лікування; та податкова, що збирає податки.

Інформація може бути пошкоджена, якщо вона доступна в незахищеній мережі. Коли інформація змінюється несподіваним чином, результат відомий як втрата цілісності. Це означає, що до інформації внесено неавторизовані зміни, будь то людська помилка або навмисне втручання. Чесність особливо важлива для критичної безпеки та фінансів дані, які використовуються для таких дій, як електронні перекази коштів, управління повітряним рухом і фінансові облік.

Інформація може бути стерта або стати недоступною, що призведе до втрати доступності. Це означає, що люди, уповноважені отримувати інформацію, не можуть отримати те, що їм потрібно.

Доступність часто є найважливішою характеристикою в державному управлінні, орієнтованому на надання послуг залежать від інформації (наприклад, розкладу нарад та онлайн-систем інвентаризації).

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[45] 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.

Ось 5 найпоширеніших кібератак:

- Шпигунське програмне забезпечення — це шкідлива програма, яка 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 троянською програмою 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.

Як бачите, багато чого може піти не так, якщо цифрові дані зламано. На щастя, безпека в цифровому світі має багато форм, пропонуючи широкий вибір методів захисту.

1.3 Основні напрямки забезпечення цифрової безпеки

Основними напрямками забезпечення цифрової безпеки інформаційних ресурсів 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 насамперед повинні бути 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:

- 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[50].

1.4 Постановка завдання

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[33] 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:

- Аналіз 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 майбутньому 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.

Висновки до розділу 1

Кібернетична безпека (кібербезпека) – стан захищеності критичних об’єктів національної інформаційної інфраструктури[1] 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 КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Як переконливо доводить світовий досвід, забезпечення можливостей у галузі забезпечення кібернетичної безпеки, що передбачає що 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.

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[11] 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.

2.1 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 [5].

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.

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.

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 доларів фінансовими й роздрібними установами [8]. 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.

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.

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[47]. *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.

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[37]* в США:

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 завдають шкоди. Ваша 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.

Проаналізовано п’ять основних напрямів діяльності з питань інформаційного захисту, які визначає Стратегія [19]: 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.

У ході дослідження виявлено такі чинники, що сприяли проведенню успішної інформаційної політики[48] 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»).

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. 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.

Кіберстрахування – захист малого та середнього бізнесу. Кіберстрахування – 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.

2.2 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[36].

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.

Рада ЄС визначила ключові напрямки діяльності із розвитку кібернетичної безпеки на наступні роки [12]. 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[41] 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 [28] 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 [13].

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:

- стійкість, технологічний суверенітет і лідерство;
- оперативні можливості для запобігання, стримування та реагування;

- 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 [9].

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.

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.

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*.

9 березня 2021 року Колегія Єврокомісії схвалила дорожню карту "Цифровий компас" – 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. 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"[39] 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[49]. Громадяни ЄС зможуть повноцінно використовувати засоби цифрової ідентифікації, мати безобмежений доступ до власних електронних даних.

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.

2.3 Формальний аналіз забезпечення кібернетичної безпеки у Європі, США та Україні

В рамках подальшого розвитку співробітництва України з США та 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:

1. Завершити створення чіткої робочої системи[31] 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 надзвичайні ситуації 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 Росії 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[43] для вирішення непрофільних завдань, в тому числі, для кібершпигунства.

Висновки до розділу 2

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. А на прикладі США у ході дослідження виявлено багато чинників, які сприяли проведенню успішної інформаційної політики. 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 міжнародно-правових та європейських норм у національне законодавство України, особливо щодо запровадження режиму кіберсанкцій[10].

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.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ ТА МІСЦЕВОГО САМОВРЯДУВАННЯ

Кіберпростір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою соціального 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 кібербезпеки, 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 [14]. З огляду на вищенаведений вислів варто визначитися з термінами. До сьогодні в публікаціях можна зустріти різні поняття, що використовуються як синоніми, зокрема, «безпека інформації», «інформаційна безпека», та «кібербезпека», автори підміняючи між собою ці поняття вводять суспільство в оману.

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. Для кваліфікації безпеки в сфері інформації мають враховуватися і інші властивості, такі як справжність (3.6), звітність, неприйняття (3.48) та надійність (3.55). В національному вимірі поняття безпека інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних.

3.1. Нормативно-правове забезпечення України

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 [16], 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» [16] 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 [27] 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. Відповідно до ДСТ України ISO/IEC 27032:2016 [27] 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 [30], 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 [2, 11], 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.

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, а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України».

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [15], правову основу кібербезпеки України становили Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» [24], 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» [15] 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 [17]:

– 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 кібербезпеки 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 кібербезпеки 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.

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» [21], 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.

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) [16] 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.

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 кібербезпеки.

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 кібербезпеки 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.

3.2. Пропозиції та перспективи в даній сфері

Очевидно, що об'єктом зацікавленості злочинців була і завжди буде приватна інформація, витоки якої здійснюють під час використання соціальних мереж через такі канали, як персональні комп'ютери, ноутбуки, смартфони, а тому необхідно прописувати правила користування цією інформацією і стежити за безумовним їх виконанням.

Не менш важливим повинно стати належне реагування на інциденти (внутрішнє чи зовнішнє – залежно від обставин). Інформування відповідних органів є способом поліпшення загальної ситуації у галузі кібербезпеки.

Рис. 3.1 Заходи щодо кіберзахисту інформації.

Одним з варіантів вирішення питання кібербезпеки є створення або спеціальної служби із забезпечення кібербезпеки, або введення посади спеціаліста з кібербезпеки, який займатиметься розробленням охоронних систем для різних комунікаційних мереж і електронних баз даних [3].

Спецслужбу з кібербезпеки можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп'ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки[44].

Обов'язками таких фахівців є:

- виявлення уразливих місць системи та моделювання можливої ситуації стороннього кібервпливу з позиції загроз і пов'язаних із ними ризиків;
- контроль надійності функціонування системи захисту облікової інформації, розроблення заходів безпеки на випадок непередбачуваних подій;
- віднесення облікової інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації);
- розроблення положень, політики і процедур у рамках системи безпеки облікової інформації;
- упровадження розроблених заходів безпеки та випробування системи з оцінкою її результативності, за необхідності внесення

коригувань;

- встановлення користувачам комп'ютерної системи бухгалтерського обліку необхідних реквізитів захисту;
- навчання користувачів комп'ютерної інформаційної системи правилам безперервної обробки інформації;
- контроль за дотриманням користувачами комп'ютерної інформаційної системи та персоналом підприємства встановлених правил роботи з обліковою інформацією, що захищається у процесі її автоматизованої обробки.

Для унеможливлення неправомірного втручання у комп'ютерну інформацію та попередження злочинів із його використанням необхідно створити належну систему захисту цієї інформації [2]. Це завдання не може бути вирішене ефективно без дотримання певних принципів (рис. 3.2).

Рис. 3.2 Основоположні принципи системи заходів кібербезпеки

Дуже важливо дотримуватись 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.

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».

3.3. Особливості роботи та приклад застосування в Україні

В реаліях, коли Україна захищає свою національну безпеку та цілісність від агресії з боку рф, кіберпростір – це стратегічно важливий фронт. Наша країна щоденно продовжує бути мішенню хакерських атак, спрямованих на державні установи критичної інфраструктури, приватний бізнес та на українських громадян. За даними Державної служби спеціального зв'язку та захисту інформації України, від початку повномасштабної війни, росія здійснила 796 кібератак проти України, що втричі більше у порівнянні з аналогічним періодом минулого року. За даними *CERT-UA* у першому півріччі 2022 року [20] було зафіксовано 1350 кібератак.

В цілому, за даними звіту від *Microsoft* , у 2021 році майже 20% усіх кібератак у світі були спрямовані проти України, що, після США, посідає друге місце в цьому «анти-рейтингу». Крім того, за минулий рік Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту зафіксував 41 млн підозрілих подій інформаційної безпеки (спроб стороннього втручання), опрацював 160 тисяч критичних подій (ставлять під загрозу захищеність та функціонування інформаційних ресурсів) та зареєстрував 147 кіберінцидентів, що мали ознаки потенційних кібератак. З них найбільша кількість стосувалися шкідливого програмного коду - тобто, програм, що перешкоджають роботі комп'ютера і отримують доступ до приватних комп'ютерних систем, (28%), збору конфіденційної інформації зловмисниками (18%) та шахрайства (6%). Як правило, атаки здійснювалися з території рф.

Не дивлячись на складну ситуацію і численні виклики кібербезпеки, Україна посіла 24 місце із 160 в рейтингу Національного індексу кібербезпеки, який щорічно складає Фонд електронного урядування Естонії. Ключовими критеріями, які впливають на оцінку країни, є наступні можливості держави:

- визначення кіберзагроз;
- створення системи захисту від них;
- розвиток відповідного освітнього напрямку для підвищення рівня обізнаності населення в сфері кібербезпеки.

У цьому списку Україна випередила частину європейських країн, зокрема: Австрію, Ірландію та Норвегію. Можемо впевнено трактувати отримані результати як досить оптимістичні, але не варто забувати, що кіберзахист нашої держави все ще має слабкі місця у протистоянні потенційним загрозам.

3.3.1 Огляд загальної ситуації на 2022 рік

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. Ця атака стала найбільш потужною за останні 4 роки. Зловмисники скористалися вразливістю системи управління контентом сайту *October* (*October-CMS*), яку використовувала компанія *Kitsoft* для розробки сайтів органів влади України. Отримавши адміністративний доступ до інфраструктури *Kitsoft[42]*, зловмисники також отримали доступ до всіх постраждалих сайтів органів влади та місцевого самоуправління. Контент сайтів та критична інфраструктура не постраждала, витоку персональних даних не біло. Більшість ресурсів відновили свою роботу 16 січня.

15 лютого о 20:21 почалася DdoS-атака на державні сайти та сайти багатьох банків України, яка відбувалася впродовж 5 годин. Атака стала найпотужнішою в історії нашої держави. Цілями в цей раз були близько 15 банків, в тому числі державні банки “Приватбанк” та “Ощадбанк”, а також сайти домену .gov.ua. Сайти на деякий час припинили роботу. Взагалі сайти банків постраждали менше, та відновили роботу вже 16 лютого. Представники Держспецзв’язку запевняють, що витоку даних не було, пошкодження або знищення елементів критичної інфраструктури також не відбулось.

23 лютого напередодні російського вторгнення близько 16:00 почалася нова масштабна DdoS-атака на сайти органів самоврядування, банків та структур безпеки України. Сайти Верховної Ради, Кабінета міністрів та СБУ припинили

роботу. За даними Blumberg, хакери знищили дані в мережі Міністерства внутрішніх справ та викачали велику кількість даних з телекомунікаційної мережі держави.

Продовж поточного року ми регулярно бачимо заяви Урядової команди реагування на комп'ютерні надзвичайні події України про активність хакерів.

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

3.3.2 Стратегія безпеки

Головною особливістю роботи українських органів управління та місцевого самоврядування можна вважати використання продуктів компанії Microsoft, таких як операційні 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[40]* рекомендує орієнтуватися на модель захисту *Zero Trust* на Рис. 3.3. Вона адаптована до складного сучасного середовища й дозволяє захищати користувачів, пристрої, програми, дані та інфраструктуру.

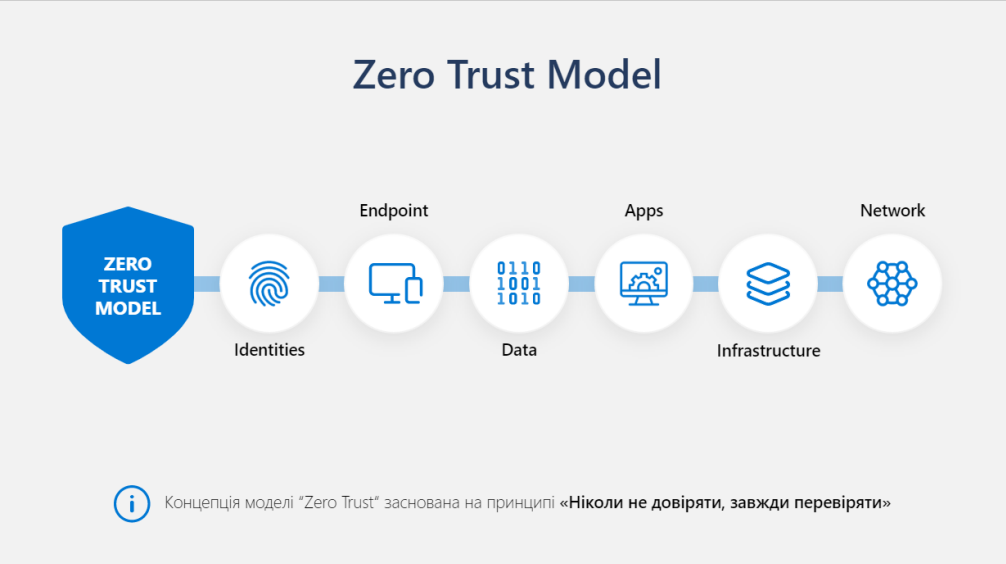

Рис. 3.3 Модель захисту Zero Trust

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.

Основний меседж *Zero Trust*: «Ніколи не довіряти, завжди перевіряти». Ця модель передбачає, що зловмисники є як всередині, так і за межами мережі, тому жодним користувачам чи пристроям не можна автоматично довіряти. Zero Trust перевіряє ідентичність та привілеї користувача, а також ідентифікацію та безпеку пристрою.

Ця модель поєднує у собі політики, практики та технологічні інструменти, які працюють разом, щоб забезпечити компаніям більш надійний рівень безпеки.

Області захисту моделі *Zero Trust*:

- *Identity* - організація перевірки та контролю ідентифікаційних даних користувачів із застосуванням суворої автентичності у всьому цифровому середовищі компанії.
- *Endpoints* - контроль усіх пристроїв, які звертаються до інфраструктури компанії. Забезпечення перевірки стану та відповідності вимогам перед наданням доступу.
- *Data* - перехід із захисту на основі периметра до системи безпеки на основі даних. Використання аналітики для класифікації та маркування даних. Організація шифрування та обмежень доступу з урахуванням політик компанії.
- *Apps* - пошук тіньових IT у своєму середовищі, контроль прав та привілеїв усередині додатків, організація доступів на основі аналітики в режимі реального часу, відстеження та контролю прав користувачів.
- *Infostructure* - використання засобів телеметрії, щоб виявляти атаки або аномалії та автоматичне блокування та маркування небезпечних дій; організація доступів з урахуванням мінімальних необхідних привілеїв.
- *Network* - недовіра до пристроїв та користувачів на підставі того, що вони знаходяться всередині мережі компанії. Організація шифрування всіх каналів обміну даними та обмеження доступу на основі політик компанії.

Кожен із цих рівнів – важлива ланка в моделі нульової довіри. І кожен із них зловмисники або самі користувачі можуть використати як точки входу чи канали для витоку корпоративної інформації[46].

3.3.3 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. 3.4). Це додає до процесу входу ще один рівень захисту.

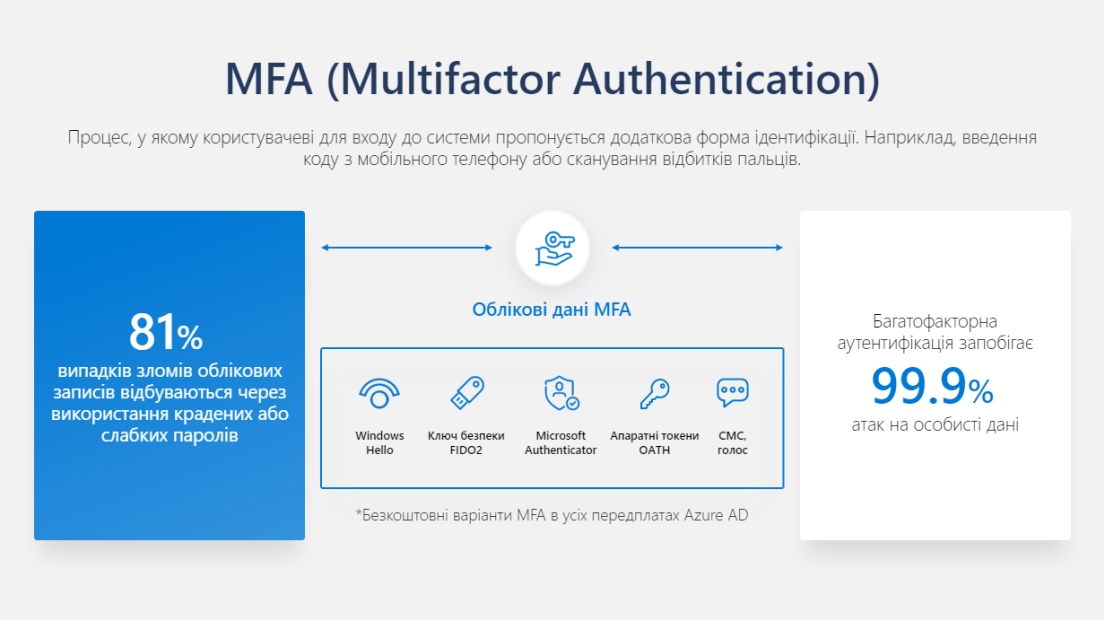

Рис. 3.4 Метод аутентифікації *MFA*

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. 3.5).

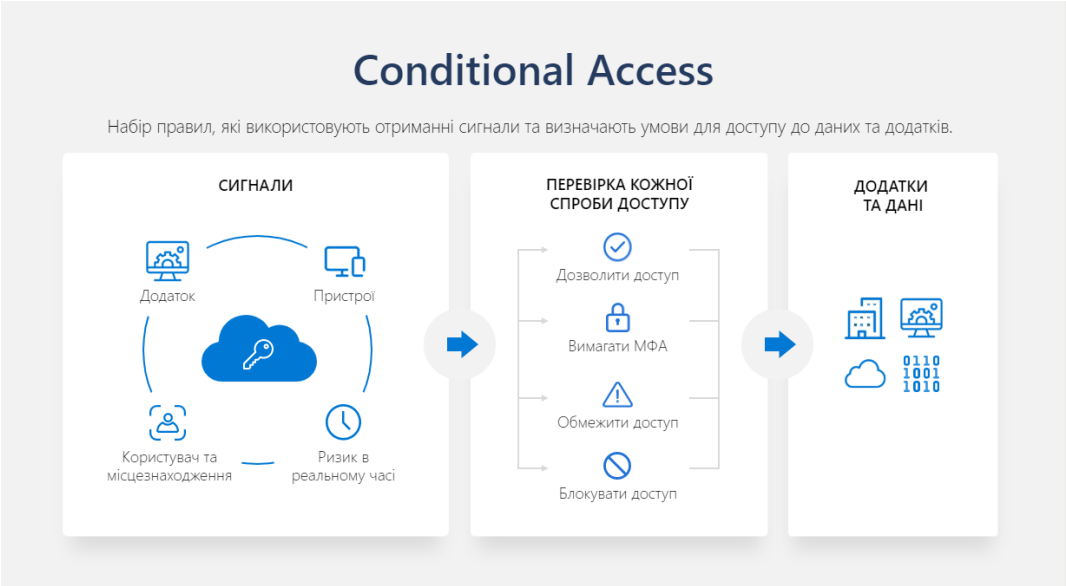

Рис. 3.5 Управління доступом *Conditional-access*

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.

3.3.4 Захист кінцевих точок

У сучасних компаніях є великий «зоопарк» 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. 3.6), дає змогу управляти мобільними пристроями *Intune (MDM)* та управляти програмним забезпеченням *Intune (MAM)*.

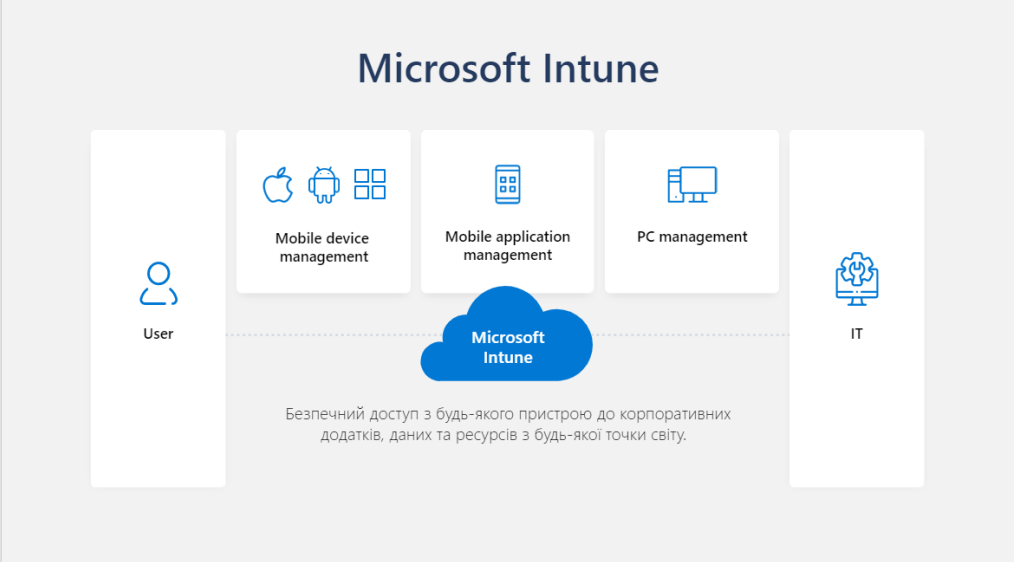

Рис. 3.6 Структура *Microsoft Intune*

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.

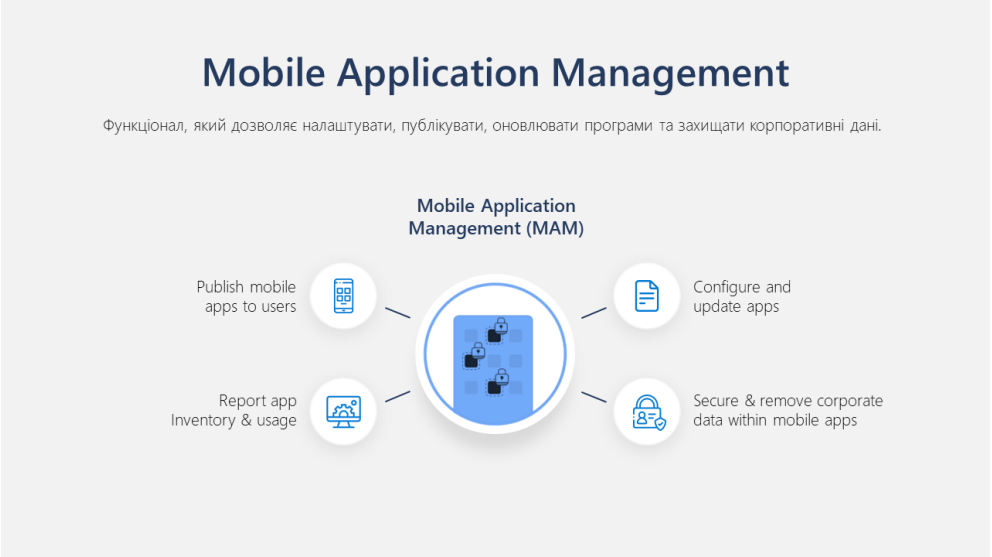

Рис. 3.7 Політики захисту *Intune MAM*

За наявності політик захисту *Intune MAM* (рис. 3.7), 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. 3.8) забезпечує централізоване керування кінцевими пристроями на платформах *Android, iOS, Windows, MacOS*.

Рис. 3.8 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 найкраще у своєму класі захисне рішення, яке 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*.

3.3.5 Безпечна робота з корпоративними даними

В умовах масштабної війни у 2022 році кількість працівників, що працюють віддалено, з домашніх офісів, стрімко зростала. За даними міжнародної дослідницької компанії IDC, більшість компаній не мають змоги забезпечити віддалений доступ через мережу VPN, яка забезпечує безпечне та зашифроване з'єднання з внутрішньою мережею компанії. Це створює ідеальні умови для атак хакерів.

Захист інформації, а також безпечна робота стають необхідними заходами для стабільного функціонування органів публічного управління, підвищення продуктивності ІТ-фахівців, надання співробітникам доступів до внутрішньої інформації та організації їхньої роботи з будь-якої точки світу.

Випадки порушення ІТ-безпеки компаній пов’язані з крадіжкою облікових даних. Ось чому одним із базових аспектів системи Zero Trust є організація процесів жорсткої перевірки ідентифікаційних даних користувачів.

Налаштування багатофакторної автентифікації, скидання паролів без участі ІТ-фахівців, призначення політик умовного доступу, автоматизація процесів виявлення та усунення загроз, реєстрація додатків у хмарній службі Azure Active Directory захищає від 99% кібератак, пов’язаних з ідентифікацією.

Ще однією небезпекою для захисту віддаленого доступу є домашній Wi-Fi. Через наявність великої кількості вразливостей на пристроях Інтернет-речей, включно з роутером, вони є популярною ціллю для зловмисників. Саме тому перед підключенням робочих ноутбуків до домашньої мережі важливо перевірити роутер на наявність вразливостей.

У будь-якому органі державної влади присутні об’єми даних, які необхідно захищати. Для цього у *Microsoft* є відповідні сервіси, які об’єднані у напрямок *Data Protection*(рис. 3.9).

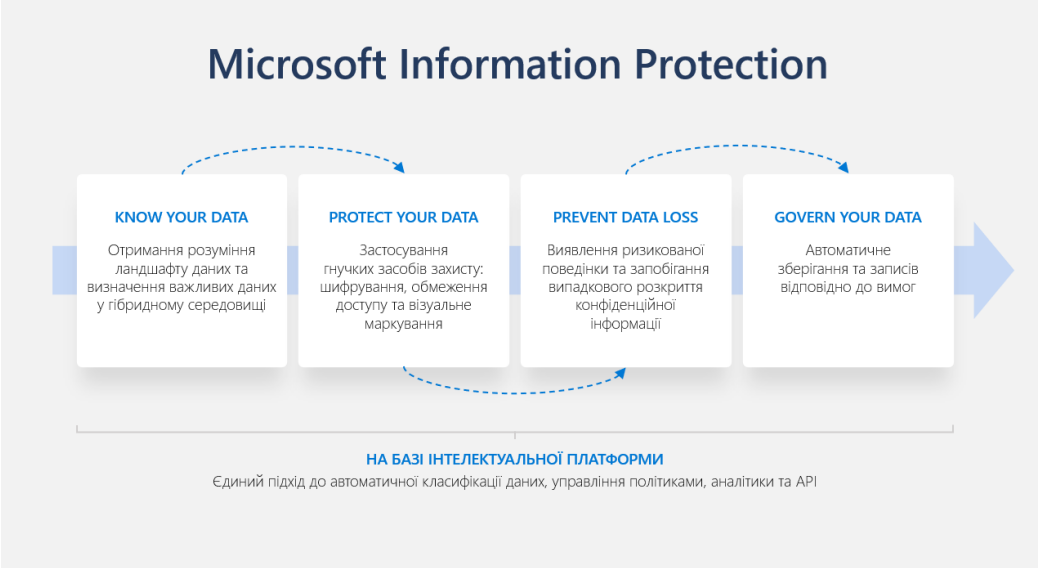

Рис. 3.9 Сервіси *Microsoft Data Protection*

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)*.

3.3.6 Захист пошти

Захист електронної пошти – це практика захисту облікових записів електронної пошти й спілкування від несанкціонованого доступу, утрати даних або порушень безпеки. Організації можуть посилити захищеність електронної пошти, застосувавши політики й інструменти для убезпечення від таких зловмисних загроз, як шкідливе програмне забезпечення, спам і фішингові атаки. Кіберзлочинці спрямовують атаки на електронну пошту, оскільки таким способом вони можуть легко отримати доступ до облікових записів і пристроїв інших користувачів. Подібні атаки трапляються здебільшого через людську

помилку. Лише одне хибне натискання може спричинити кризу безпеки для цілої організації.

У відповідь на мінливі загрози підприємства розробили практичні поради щодо захисту електронної пошти, щоб підтримувати спілкування й убезпечити себе від кібератак.

Служби захисту електронної пошти допомагають компаніям убезпечувати облікові записи електронної пошти та спілкування від кіберзагроз. Найкращий спосіб для компаній захистити електронну пошту – створити й застосувати політику її використання, якою вони поділяться з працівниками, щоб ті були поінформовані про рекомендації щодо безпеки. Нижче наведено можливості найпоширеніших служб захисту електронної пошти, які доступні для окремих користувачів, навчальних закладів, спільнот і організацій.

Ми 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 я рекомендую 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 ваші 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.

3.3.7 Виявлення потенційно небезпечних програм

Для розуміння основного тлумачення виявлення потенційно небезпечних програм розтлумачимо поняття проактивного захисту, а саме це сукупність технологій, яка використовується в антивірусному програмному забезпеченні, головною метою яких є виявлення потенційно небезпечного програмного забезпечення. На відміну від сигнатурних технологій, вони попереджають, а не виявляють вже відоме зловмисне програмне забезпечення в системі. При цьому проактивний захист намагається блокувати потенційно небезпечну активність програми. Великим недоліком проактивного захисту є хибні спрацьовування, внаслідок чого блокуються легітимні (нешкідливі) програми.

Для виявлених потенційно небезпечних програм потрібно прогнозувати сценарії виникнення і розвитку можливих аварій, що призводять до реалізації потенційних небезпек. Сценарій має починатися з події (стадії), що утворює безпосередню загрозу виходу процесу з-під контролю й виникнення аварії.

Під час аналізу небезпеки інформаційного ресурсу потрібно визначити всі можливі аварійні ситуації і можливі ураження, в тому числі й малоймовірні, з катастрофічними наслідками, які можуть виникати як в місцевих органах та інших орагнах державної влади , розглянути сценарії їхнього розвитку і оцінити наслідки.

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.

Категорії програмного забезпечення(далі - ПЗ), які можна розглядати як умовно шкідливе: ПЗ, що відображає рекламу або виконує завантаження інших програм, різноманітні браузерні панелі інструментів, ПЗ з оманливою поведінкою, пакетне ПЗ, ПЗ для відстеження користувацьких операцій, майнери криптовалют, програми для очищення реєстру (тільки в операційних системах Windows), будь-яке інше сумнівне ПЗ або програмне забезпечення із застосуванням противоправних або принаймні неетичних практик ведення бізнесу (незважаючи на те, що його використання може сприйматися як правомірне), яке кінцевий користувач може розцінити як небажане, коли він або вона дізнається про особливості роботи цього ПЗ після інсталяції.

В *Microsoft Defender for Cloud Apps* є інструменти, які допомагають виявляти тіньові IT-ресурси (Shadow IT) (рис. 3.10) та оцінювати ризики, а також дозволяють застосовувати необхідні політики безпеки та проводити розслідування інцидентів.

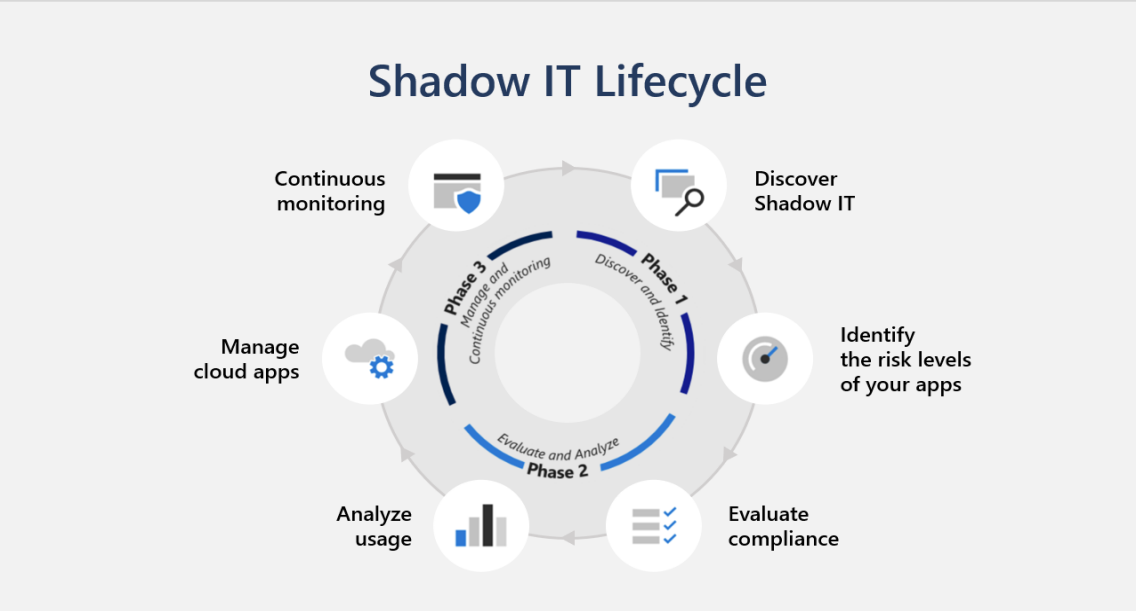

Рис. 3.10 IT-ресурси *Shadow IT*

3.3.8 Організація безпечної роботи в хмарі

Усі, хто вже частково або повністю перемістив свій ресурс у хмару, розуміють, що цього, на жаль, недостатньо. Якщо не занурюватися глибоко в тему, може здатися, що проблема досить надумана. Дійсно, яка різниця, де розташовується сервер, якщо це ті самі Windows Server або Linux. Встановлюємо звичний антивірус, IPS/IDS, підключаємо до SIEM – і готово. Але хмарна інфраструктура влаштована і працює інакше, а ще у багатьох випадках доводиться мати справу з гібридним середовищем, коли є фізичні, віртуальні та хмарні сервери.

Звичайно, засіб захисту інформації сам по собі мусить бути надійним і безвідмовним при аваріях систем. Коли віртуальна машина виходить із ладу, всі налаштування та правила повинні зберігатися.

Отже, сучасна система захисту інформації передбачає комплекс заходів: міжмережевий екран, безагентний антивірус та обов'язково систему виявлення вторгнень. Саме вона має інтегрувати захист ресурсів у хмарі та в центрі даних користувача, надавати можливість аналізу логів подій безпеки для виявлення складних багатовекторних атак та аудиту.

Інфраструктура державних органів — 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. 3.11) дає можливість захищати більшу кількість робочих процесів для таких хмарних платформ, як *Amazon Web Services (AWS) та Google Cloud Platform (GCP)*.

Публічні хмари більш «загартовані» проти зломів – хакери знають, де знайти самі «смачні» речі – звичайно ж всередині публічної хмари, де зберігається інформація багатьох клієнтів. Якщо б вони змогли прорвати «оборону» публічної хмари, вони б отримали дуже багато всього. Тому на неймовірній кількості хакерських спроб такі великі хмарні сервіси, як Amazon Web Services, Microsoft Azure та інші – загартовуються вже на протязі багатьох років.

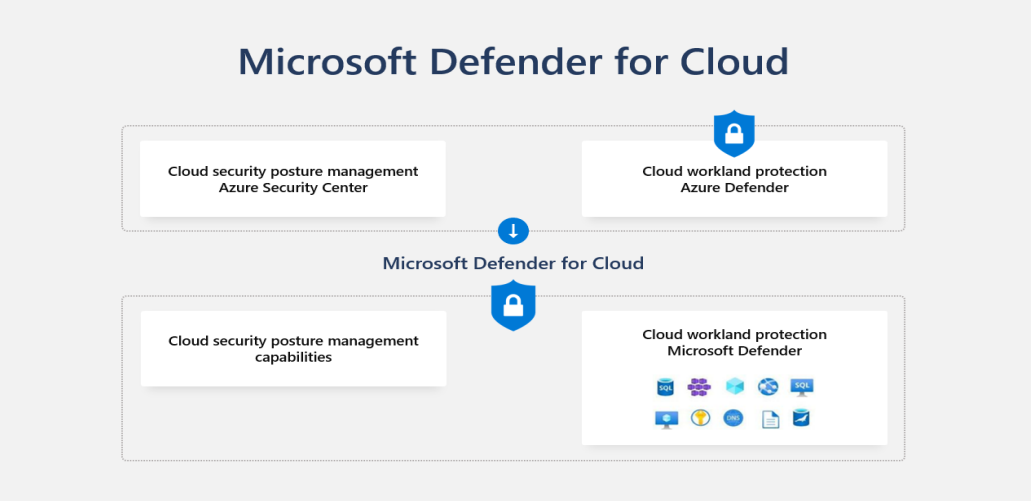

Рис. 3.11 Захист хмарних платформ *Microsoft Defender for Cloud*

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

3.3.9 Безпечний доступ до корпоративної мережі

Під корпоративною мережею розуміють комп'ютерну мережу, що об'єднує різнорідні локальні мережі. Поява і розвиток корпоративних мереж зв'язана з великою різноманітністю локальних мереж і необхідністю об'єднання їх в загальну мережу. Так, в рамках промислового підприємства, як правило, існує кілька типів локальних мереж, одні з них орієнтовані на управління виробничими процесами, інші – на обслуговування адміністративно-господарських служб. Використовувати однорідну мережу для вирішення комплексу всіх задач недоцільно, а в більшості випадків і досить важко.

В даний час існує ряд пристроїв, з допомогою яких здійснюється об'єднання різноманітних комп'ютерних мереж між собою. До таких пристроїв належать мости, шлюзи, маршрутизатори. Сама назва міст підкреслює, що об'єднуються протилежні сторони будь-чого, в нашому випадку – це локальні мережі. Таким чином, в комп'ютерних мережах міст – пристрій, що об'єднує різнорідні мережі. Характерною рисою моста є його здатність здійснювати вибіркову трансляцію (фільтрацію) блоків даних з однієї мережі в іншу на основі аналізу адрес блоків даних, що поступають. При необхідності здійснюється

перетворення форматів даних, які передаються. Тим самим проводиться розподіл інформаційних потоків в рамках корпоративної мережі. Ця властивість моста часто використовується для зниження потоку даних в комп'ютерних мережах.

Корпоративна мережа - система, що забезпечує передачу інформації між різними програмами, що використовуються в системі корпорації. Корпоративною мережею вважається будь-яка мережа, що працює за протоколом TCP/IP і використовує комунікаційні стандарти Інтернету, і навіть сервісні програми, які забезпечують доставку даних користувачам мережі. Наприклад, місцевий орган може створити сервер Web для публікації оголошень, виробничих графіків та інших службових документів. Службовці здійснюють доступ до документів за допомогою засобів перегляду Web.

Місця, де корпоративна мережа підключається до Інтернету, є периметром безпеки мережі. У цих точках перетинається вхідний і вихідний трафік. Трафік корпоративних користувачів виходить за межі мережі, а інтернет-запити від зовнішніх користувачів для отримання доступу до веб-додатків і додатків електронної пошти входять в мережу компанії.

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.

Завдяки продуктам Microsoft забезпечується повна доступність брандмауера і сервісів VPN. Функції брандмауера забезпечують фільтрацію рівня додатків зі збереженням стану для вхідного і вихідного трафіку, захищений вихідний доступ для користувачів і мережу DMZ для серверів, до яких необхідно здійснювати доступ з Інтернету.

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 до розділу 3

Сучасний світ як ніколи оснащений великою кількістю засобів зв'язку. Світову економіку формують люди, які спілкуються, перебуваючи в різних часових поясах, і отримують доступ до важливої інформації звідусіль. Кібербезпека стимулює продуктивність і впровадження інновацій, що дає користувачам змогу впевнено працювати та спілкуватись онлайн. Правильні рішення й процеси дають змогу компаніям і державним установам користуватися технологіями для покращення спілкування та надання послуг, не ризикуючи постраждати від атак.

На жаль, кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загально державного рівня, а кожного окремо взятого підприємства. Зрозуміло, що неможливо досягти стовідсоткової безпеки захисту облікових даних.

Проте індивідуальна відповідальність кожного працівника є найпершим і найпростішим фактором, який сприяє захисту цінної облікової інформації. Таким чином, на кожному підприємстві повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації, сфера застосування якого поширюється на людські ресурси і не обмежується винятково технологічними аспектами.

Оскільки все більше організацій упроваджують моделі гібридної роботи, що дають робітникам змогу працювати як в офісі, так і віддалено, варто розгортати нову модель безпеки, яка захищатиме користувачів, пристрої, програми та дані, хоч де вони зберігатимуться. Принцип інфраструктури з моделлю нульової довіри полягає в тому, що більше не можна довіряти запиту на доступ, навіть якщо він надходить із внутрішньої мережі. Щоб знизити ризик, потрібно припустити, що захист зламали, і перевіряти всі запити на доступ. Надавати користувачам доступ до потрібних їм ресурсів лише з мінімальними правами.

За кібербезпеку відповідають не лише фахівці з безпеки. Сьогодні робочі й особисті пристрої використовуються по черзі, а багато кібератак починаються з надсилання фішингового електронного листа працівникам. Навіть великі забезпечені ресурсами компанії стають жертвами соціотехнічних кампаній. Боротьба з кіберзлочинністю й убезпечення мережі вимагає спільних зусиль усіх працівників. Необхідно проводити регулярне навчання команди, щоб вона могла захищати особисті пристрої та розпізнавати й зупиняти атаки. Обов’язкове відстеження ефективність програм, використовуючи симуляції фішингу.

Важливо розгортайте процеси, які допоможуть запобігати атакам, а також виявляти й усувати їх. Регулярно оновлювати програмне й апаратне забезпечення, щоб зменшити кількість вразливостей, і надавати працівникам чіткі вказівки щодо дій у разі атаки.

Технологічні рішення, які допомагають усувати проблеми з безпекою, щороку вдосконалюються. Багато рішень із кібербезпеки використовують штучний інтелект і автоматизацію, щоб виявляти та зупиняти атаки без втручання відповідних фахівців. Завдяки деяким технологіям можна аналізувати робоче середовище й отримувати відповідну аналітику. Комплексні рішення для кібербезпеки дають змогу мати повну картину робочого середовища й усувати прогалини в безпеці. Вони працюють синхронізовано з екосистемою та захищають ідентичності, кінцеві точки, програми й хмари.

ВИСНОВКИ

У магістерській роботі наведено теоретичне узагальнення і нове вирішення наукової проблеми, яке виявляється у визначенні сутності, особливостей забезпечення кібербезпеки інформаційних ресурсів органів публічного управління та місцевого самоврядування в Україні, що дозволило сформувати відповідну наукову концепцію, а також обґрунтувати низку нових положень і рекомендацій щодо подальших напрямків і перспектив функціонування та розвитку зазначеної теми.

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 та слідуючи у ногу з організації кіберзахисту країн партнерів.

Згідно завдань роботи отримано наступні результати:

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

– проведено аналіз цифрової трансформації публічного управління в умовах кібернетичного захисту інформаційних ресурсів державних органів;

– проведено аналіз концепцій цифрової безпеки у сучасному світі з розтлумаченням основних можливих загроз кібернетичного простору державного сектору управління;

– визначено основні напрямки забезпечення цифрової безпеки та постановки завдання на основі проведеного аналізу кібернетичної безпеки в публічному управління;

– проаналізовано досвід країн партнерів(США, ЄС), що забезпечують швидкий, зручний та надійний спосіб забезпечення кібербезпеки інформаційних

ресурсів між різнорівневими органами управління та самоврядування в Україні, щодо завдання кіберзахисту;

– проведено формальний аналіз забезпечення кібернетичної безпеки у Європі, США та Україні в умовах кібернетичного захисту інформаційних ресурсів в органах державного управління;

– виконано дослідження та проаналізовано нормативно-правову складову в сучасних умовах;

– визначено перспективи та пропозиції у сфері кібернетичного захисту інформаційних ресурсів органів державного управління;

– запропоновано можливі технічні рішення у даній сфері для зменшення витрат часу на виконання поставлених завдань;

– визначено подальші напрямки роботи.

З'ясовано призначення 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.

Важливе значення для розвитку забезпечення кібербезпеки інформаційних ресурсів даних органів 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 цього та інших напрямків, інформаційні ресурси органів публічного управління та місцевого самоврядування повинні мати ефективні та зручні у використанні програмні засоби, що постійно розвиваються та оновлюються.

Поставлені завдання дослідження виконані, мета роботи досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аванесова Н. Е., Мордовцев О. С., Сергієнко Ю. І. Теоретико-методичні засади ідентифікації та взаємозв'язку впливу дестабілізуючих факторів на економічну безпеку промислового підприємства. Бізнес Інформ. 2020. №9. С. 20–28. DOI: https://doi.org/10.32983/2222-4459-2020-9-20-28
2. Азарова А. О. Електронні засоби політики інформаційної безпеки на державних підприємствах [Електронний ресурс] / А. О. Азарова, В. Ф. Хісматулліна // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані. – 2019. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/view/6889.
3. Азарова А. О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу [Електронний ресурс] / А. О. Азарова, В. О. Гудзь, В. О. Блонський // Матеріали XLVIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 13-15 березня 2019 р. – Електрон. текст. дані.
4. Баранов О. А. Про тлумачення та визначення поняття "кібербезпека". Правова інформатика . 2014. № 2 (42). С. 54–62
5. Бірюков Д.С. Зелена книга з питань захисту критичної інфраструктури в Україні / Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт, О.М. Суходоля – К. : НІСД, 2015. – 35 с.
6. Великий тлумачний словник сучасної української мови / Гол. ред. В. Т. Бусел. – К. : Ірпінь: ВТФ «Перун», 2005. – 1728 с.
7. Використання інформаційних та комунікаційних технологій в сучасному цифровому суспільстві : колективна монографія. - Херсон : Вишемирський В. С., 2020. - 148 с

8. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. Безпека інформації.2013. Т. 19, № 2. С. 118–129.
9. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С. Ф. Гончар ; НАН України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. - Київ : Альфа Реклама, 2019. - 175 с.
10. Дзюндзюк В. Б. Публічне управління в Україні: рух з минулого у майбутнє // Актуальні проблеми державного управління. – 2019. – № 1. – С. 8-18.
11. Діордіца І. В. Поняття та зміст національної системи кібербезпеки URL: http:// goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/.
12. 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*
13. Європейське агентство з мережевої інформаційної безпеки (ENISA), 201 [Електрон. ресурс]. – Режим доступу: *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss*
14. Закон України «Про Національну програму інформатизації» від 01.08.2016р. № 74/98-ВР. // [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
15. Закон України «Про основні засади забезпечення кібербезпеки України» від 17.08.2022
16. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. № 537-V
17. Логінова Н. І. Правові основи кібербезпеки в Україні. Правові та інституційні механізми забезпечення розвитку держави та прав в умовах євроінтеграції: матеріали міжнар. наук.-практ. конф. Одеса: 2016. Т. 1. С. 575–577.
18. Мінін Д.С. Підходи до визначення поняття «кібербезпека» / Д.С. Мінін [Електронний ресурс]. – URL : http://istfak.org.ua/tendentsii-rozvytkusuchasnoi-systemy-mizhnarodnykh-vidnosyntasvitovohopolitychnoho-protsesu/185-

heopoli-tychna-dumka-taheostratehichni-protsesy-v-khkhi-st/971-pidkhody-dovyznachennya-ponyattya-kiberbezpeka.

19. Передерій Т. С. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. Вісник економічної науки України. 2019. № 2 (37). С. 201-204. doi: https://doi.org/10.37405/1729-7206.2019.2(37).201-204
20. Перший щорічний звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [Електронний ресурс] .– Режим доступу URL: https://cert.gov.ua/article/17696
21. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», № 991 від 02.09.2022
22. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2939-17.
23. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/851-15.
24. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
25. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2297-17.
26. Публічне управління та адміністрування в умовах інформаційного суспільства: вітчизняний і зарубіжний досвід : монографія / Запоріз. держ. інж. акад. ; за заг. ред. Сергія Чернова [та ін.]. - Запоріжжя : ЗДІА, 2017. - 602 с.
27. Стандарт ICO/IEC 27032

28. Ткачук Н.В. Стан та проблемні питання реалізації Стратегії кібербезпеки України. Інформація і право. № 1(28)/2019. С. 129-134.
29. Указ Президента України №447/2021 від 14 травня 2021 року "Про Стратегію кібербезпеки України";
30. Хлапонін Юрій І. та ін. Аналіз стану кібербезпеки в провідних країнах світу. Кібербезпека: освіта, наука, техніка, 2019, 4.4: 6-13.
31. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 1 (27). С. 312–320.
32. *Brendan Burns - Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Services. O'Reilly Media; 1ie ed. 2018. - 166 pages*
33. *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/
34. *Cyber Security Strategy Documents. URL: https://ccdcoe.org/strategies-policies.html*;
35. *Cybersecurity and Infrastructure Security Agency Act of 2018. URL: https://www.congress.gov/bill/115th-congress/house-bill/3359*
36. *Europe's Digital Decade: Digitally empowered Europe by 2030. URL: https://ec.europa.eu/*
37. *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*
38. *Karpenko, O. V., Arsenovych, L. A. (2020). State cyber education and tools to increase the level of digital competence of the population of Ukraine. Visn. NADU. Seriia «Derzhavne upravlinnia», № 1 (96), s. 95–102.*
39. *Martin, A., Grudziecki, J. (2006). Concepts and Tools for Digital Literacy Development. Innovations in Teaching and Learning inInformation and Computer Sciences, vol. 5, no. 4, pp. 246-264.*

40. *Microsoft Digital Defense Report [Електронний ресурс] .– Режим доступу URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi*
41. *MinV&J (2011b) The National Cyber Security Strategy (NCSS): Success Through Cooperation, Netherlands Ministry of Security and Justice, The Hague, Netherlands, available at http://www.enisa.europa.eu/media/newsitems/dutch-cyber-security-strategy-2011.*
42. *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*
43. *ROADMAP: Proposal on a European Strategy for Internet Security http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_europe an_i nternet_security_strategy_en.pdf*
44. *The Administration's Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-protect-critical-infrastructure;*
45. *The benefits of Cyber Insurance. URL: https://www.loricainsurance.com/legacy/documents/Summary - Cyber.pdf.*
46. *The Department of Defense Cyber Strategy. URL: strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf;*
47. *US-CERT: Understanding Hidden Threats: Rootkits and Botnets. URL: https://www.us-cert.gov/ncas/tips.*
48. *Waltz, Kenneth N. Theory of International Politics. Reading, MA: Addison-Wesley Pub., 1979.*
49. *Waxler, C. CIOs Struggle with Social Media's Security Risks, Public CIO, February 11, 2011.*
50. *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*