МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВІДОКРЕМЛЕНИЙ ПІДРОЗДІЛ «МИКОЛАЇВСЬКА ФІЛІЯ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ КУЛЬТУРИ І МИСТЕЦТВ»

Кафедра інформаційної, бібліотечної та архівної справи

Допущено до захисту

_____

Протокол №_____від «__»_____р.

«СТРАТЕГІЇ РОЗВИТКУ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ»

Кваліфікаційна робота
студентки 4 курсу,
групи ІБАС-28М
Мохової Карини Сергіївни

Науковий керівник:
кандидат педагогічних наук, доцент
Шуляк Світлана Олександрівна

Миколаїв – 2022

З М І С Т

ВСТУП

Актуальність теми дослідження. Швидкий розвиток ІТ-технологій поступово трансформує світ. На даний момент кіберпростір розглядається як важливий безпековий імператив, оскільки від його реалізації залежать економічна, військова, соціальна та інші сфери діяльності держави. Кіберпростір розширює свободу і можливості людей збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поширюються випадки незаконного створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет.

Кіберзлочинність стає міжнаціональною та здатна завдати шкоди інтересам особи, суспільства і держави в цілому.

Це зумовлено тим, що сфера Інтернету, електронних послуг,інформаційних технологій стали невід’ємною часткою економіки всього світу: від цифрового документообігу, інтернет-магазинів та онлайн-банкінгу до системи цифрового управління підприємствами.

Система кібербезпеки повинна працювати в інтересах суспільства як для постачальників, так і для користувачів послуг. Саме держава як гарант прав і свобод громадян має взяти на себе відповідальність за забезпечення доступу до стабільного безпекового цифрового простору, яким можуть користуватися всі громадяни, адже забезпечення гідного рівня кібербезпеки є необхідною умовою розвитку інформаційного суспільства.

Отже, актуальність теми дослідження полягає у висвітлення основних аспектів кібернетичного простору України; визначення кібербезпеки як

складової частини інформаційної безпеки; аналізу правового забезпечення у сфері кібербезпеки України; показ основ кіберзлочинності в інформаційному просторі (види, типи, поняття, класифікація кіберзлочинів та кібератак); висвітлення особливостей запобігання кіберзлочинності; розгляду стратегічних напрямків розвитку кіберзахисту в інформаційному просторі України, для запобігання незаконних злочинів в цифровій сфері.

Стан наукової розробленості теми дослідження свідчить про те, що аспекти вітчизняних проблем у інформаційній та кібербезпеці досліджувалися у наукових працях І.В. Арістова, І.Р. Березовської, Р.А. Калюжного, Б.А. Кормича, В.А. Ліпкана, А.І. Марущак, В.С. Цимбалюка, О.К. Юдіна та інших.

Питанням правового забезпечення протидії загрозам у кібернетичній сфері присвятили свої праці такі науковці, як: І.В. Сопілко, Д.С. Мінін, В.П. Шеломенцев, В.Л. Бурячок, С.С. Горовий, І.В. Діодріца та інші.

Варто відзначити, що наукові праці Д.Дубова, присвячені стратегічним напрямкам кібербезпеки України. Важливість питання інформаційної та кібернетичної безпеки України та механізми їх формування приділяли увагу, так Д.С. Безуглий висвітлив необхідність інформаційної безпеки як компонента національної безпеки країни.

Дослідженню поняття та змісту національної системи кібербезпеки присвячено праці В.А. Ліпкана, О.О. Черноногa, О.А. Баранова, О.Ю. Запорожець, В.П. Шеломенцева, В.В. Куцаєва, Є.О. Живило, Ю.О.Черниш, В.В. Петрова. Узагальнення проаналізованих робіт науковців дає можливість поглибити знання щодо окресленої теми, виявити основні шляхи її подолання.

Метою дослідження є теоретичні основи стратегії розвитку кібербезпеки в інформаційному просторі України.

Виходячи з мети дослідження, були поставленні такі **завдання**:

1. Охарактеризувати поняття кібербезпеки, через дослідження національних стратегічних документів різних країн світу та України.

2. Визначити місце кібербезпеки в інформаційному просторі України.

3. Дослідити правову базу регулювання кібернетичної безпеки України.

4. Охарактеризувати та виявити види кіберзлочинів.

5. Дослідити типи кіберправопорушників.

6. Визначити особливості заподіяння загроз кіберзлочинності.

7. Охарактеризувати стратегічні цілі формування національної системи кібербезпеки України.

8. Проаналізувати пріоритети забезпечення кібербезпеки України.

Об'єктом дослідження є кібербезпека України.

Предметом дослідження є стратегії розвитку кібербезпеки в інформаційному просторі України.

В ході дослідження були використанні такі загальнонаукові **методи** : аналіз і синтез, порівняльний аналіз, термінологічний аналіз, історичний, логічний, термінологічний, системний, функціональний, структурний, ситуаційний, адміністративний, конвергентний підходи. За допомогою, яких було визначено певні аспекти понять «інформаційна безпека», «кібербезпека» та інші; історичне формування кібербезпеки в Україні та світі; проведенні дослідження у сфері інформаційного простору; було здійснено порівняльний аналіз термінів кіберзлочинів та кібератак, визначивши їх класифікацію; здійснено комплексний аналіз правової бази у сфері кібербезпеки.

В кваліфікаційній роботі під час проведення досліджень були, також використанні спеціальні методи, такі як, метод контент-аналізу; метод дослідження документних потоків; методи історичного дослідження (історично-порівняльний аналіз); джерелознавчі методи (виявлення і добір джерел; класифікація джерел). За допомогою цих методів було упорядковано зміст роботи; здійсненний історичний аналіз кібербезпеки як складової частини інформаційного простору; систематизовано та впорядковано основний виклад роботи; було здійснено добір джерел – це праці таких відомих науковців В.А. Ліпкана, О.О. Чернонога, О.А. Баранова, О.Ю. Запорожець, В.П. Шеломенцева, В.В. Куцаєва, Є.О. Живило, Ю.О.Черниш, В.В. Петров, що розглядали сферу

кібербезпеки.

Апробацією результатів кваліфікаційної роботи є участь у науково-практичних конференціях, таких як, VI Міжнародній науково-практичній конференції «Стан та перспективи розвитку культурологічної науки» з темою доповіді «Фактчекінг як інструмент боротьби з фейками», Всеукраїнській науково-практичійа конференції здобувачів вищої освіти і молодих учених «Культурологічні трансформації XXI ст.: від теорії до практики» з темою доповіді «Інформаційна безпека та її місце в системі національної безпеки України».

Структура кваліфікаційної роботи. Структура кваліфікаційної роботи зумовлена метою і завданнями дослідження, логікою подання матеріалів і висновків. Вона складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел.

Загальний обсяг – 72 сторінки: основний текст – 62 сторінки, список використаних джерел – 64 найменування. Оригінальність тексту кваліфікаційної роботи – 94 %.

РОЗДІЛ 1. КІБЕРБЕЗПЕКА ЯК КОМПОНЕНТ ІНФОРМАЦІЙНОГО ПРОСТОРУ

1.1. Кібербезпека: поняття та сутність

В останні роки збільшується попит на використання у різних сферах життєдіяльності суспільства цифрових та телекомунікаційних технологій, у тому числі Інтернет-комунікацій, з великою кількістю переваг принесло також невеликі загрози. Це призвело до необхідності розв'язання проблеми мінімізації сукупностей загроз. З цим і виникає термін «кібербезпека».

Поняття «кібербезпеки» досліджувалося у наукових працях І.В. Арістова, І.Р. Березовської, О.П. Дзьобаня, Р.А. Калюжного, Б.А. Кормича, В.А. Ліпкана, А.І. Марущак, В.С. Цимбалюка, О.К. Юдіна, О.О. Черноногa, О.А. Баранова, О.Ю. Запорожець, В.П. Шеломенцева, В.В. Куцаєва, Є.О. Живило, Ю.О. Черниш, В.В. Петрова, В.Л. Бурячок, С.С. Горовий, І.В. Діодріца та інших.

Уперше термін «кібербезпека» з’явився у середині 1990-х років, в США. З цього часу було організовано та проведено багато міжнародних і національних форумів, конференцій, семінарів на всіх рівнях, опубліковано велику кількість наукових робіт, присвячених різноманітним аспектам кібербезпеки. Велика кількість країн прийняли та розробляють стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших) [23, С.38].

Розглянемо, стратегії кібербезпеки різних країн світу для розуміння сутності поняття «кібербезпека». Стратегія кібербезпеки Франції, надає таке визначення: кібербезпека – це бажаний стан інформаційної системи, в якому вона може протистояти подіям з кіберпростору, які можуть поставити під загрозу доступність, цілісність або конфіденційність зберігаються, оброблюваних або переданих даних і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними. Кібербезпека використовує методи захисту інформаційних систем і заснована на боротьбі з кіберзлочинністю, і створенні кіберзахисту

[4, С.21].

У німецькій стратегії стверджується, що кібербезпека є бажаною в сфері інформаційної безпеки, при якій ризики глобального кіберпростору зведені до прийнятного мінімуму. В цілому кібербезпека розуміється, як сукупність відповідних і адекватних заходів, при яких зменшуються ризики проникнення кіберзлочинців. Також у стратегії пояснюється, що кібербезпека повинна базуватися на комплексному підході. Це має дозволити здійснити практичні кроки щодо забезпечення кібербезпеки. Про це свідчить зміст десяти стратегічних напрямів у стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини [2, С.15].

В канадській стратегії пояснюється, що стратегічним напрямком сучасного використання кіберпростору є необхідність передбачати та протистояти кіберзагрозам, що виникають. У нормативно-правовому акті не міститься чіткого визначення сутнісного змісту поняття кібербезпеки, але відносно до цієї стратегії під кібербезпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак [1].

У Турецькій Республіці національна стратегія кібербезпеки надає таке визначення поняття: кібербезпека – це захист інформаційних систем, що становлять кіберпростір, від атак, забезпечення конфіденційності, цілісності та доступності інформації, оброблюваної в цьому просторі, виявлення атак і інцидентів кібербезпеки, введення в дію контрзаходів проти цих інцидентів і подальше приведення цих систем в стан, що передує інциденту кібербезпеки [5, С.9].

В Нідерландах також беруть до уваги можливі загрози в інформаційній інфраструктурі за умов широкого застосування ІТ-технологій. У 2013 році Національним координатором з безпеки та боротьби з тероризмом була опублікована Національна стратегія кібербезпеки. На думку авторів стратегії, кібербезпека – це сукупність заходів щодо запобігання шкоди, заподіяної порушенням, збоєм або неправильним використанням ІКТ і для відновлення в

разі пошкодження [41, С. 9].

Ціллю стратегії кібербезпеки Австралії є підтримка безпечної, стійкої та надійної роботи електронного операційного середовища, яке підтримує національну безпеку Австралії та мінімізує переваги електронної економіки. В опублікованій у 2009 році стратегії під кібербезпекою розуміється забезпечення доступності, цілісності та конфіденційності ІКТ Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації [3].

В Україні також запропоновано свій варіант визначення поняття кібербезпеки, під яким розуміється стан захищеності життєво важливих інтересів людини та громадянина, суспільства і держави в кіберпросторі [9, С 56].

Виходячи з викладеного матеріалу, кібербезпека – це інформаційна безпека в умовах використання цифрових систем та телекомунікаційних мереж. Для того, щоб розуміти всю сутність значення кібербезпеки, потрібно розглянути виникнення сфери кіберпростору, тобто звідки і за яких умов він виник.

На початку XXI ст. у світі формується принципово нове, унікальне середовище, що тісно пов’язане з проникненням новітніх технологій та глобальної мережі Інтернет у наше життя – кіберпростір. Кіберпростір виник на основі комп’ютерних, мережевих, телекомунікаційних та інформаційних систем і являє собою віртуальний простір, який надає змогу здійснювати ефективну комунікацію у сфері суспільних відносин через існування сумісних між собою комунікаційних систем з допомогою електронних ресурсів та мережі Інтернет, а також інших ймовірних мереж передачі інформації. Саме таке визначення поняття кіберпростору міститься в Законі України № 2163-VIII від 05 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України».

Так, дослідник Є.В. Скулиш стверджує, що саме через сумніви щодо можливості застосування поняття кіберпростору на практиці у багатьох системах національних законодавств провідних країн світу не виділяються окремі законодавчі акти для його захисту та регулювання, а натомість

використовуються традиційні законодавчі акти. В.М. Фурашев, доповнюючи думки Є.В. Скулиша, пояснює, що під кіберпростором розуміється «форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на породження, сприйняття, запам'ятовування, перероблення та обмін інформацією». Тим самим вчений ототожнює кіберпростір та віртуальний світ, який, ґрунтуючись на реальній, матеріальній основі, має складні та неоднозначні наслідки свого функціонування та розвитку [36, С.44].

В Сполучених Штатах Америки в Національній військовій стратегії є таке визначення кіберпростіру «сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язаної з ними фізичної інфраструктури». Відносно цього Дж.Ліпман стверджує, що подібний підхід є характерним саме для фахівців з Міністерства оборони США. В останній час відбувається незначна зміна цієї точки зору, зокрема з-поміж військових спеціалістів, у бік розуміння кіберпростору як цифрового поняття [13, С.118].

В українському законодавстві кіберпростір – це середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [9, С. 56].

На даний час кіберпростір став одним із важливих складових інформаційного простору та ареною ведення справжніх війн у цифровому середовищі. Тому кібербезпека є основним елементом регулювання кіберпростору і водночас системи національної безпеки країни. Виходячи з цього розглянемо, визначення системи кібербезпеки.

Система кібербезпеки визначається як сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються.

Організація системи кібербезпеки полягає в цілеспрямованій діяльності

суб'єктів забезпечення кібербезпеки, пов'язаних зі:

– створенням і впорядкуванням організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

– налагодженням процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень [62, С.301].

Підсумовуючи можна стверджувати, що кібербезпека є найважливішим елементом у системі національної безпеки кожної держави, мета якої полягає у забезпеченні безпеки кіберпростору. Відповідний рівень захищеності є необхідною умовою функціонування та розвитку сучасного інформаційного суспільства. Ще досі питання захисту цифрового середовища є проблемним, оскільки ефективність і злагодженість взаємодії компонентних органів та інструкцій з громадськістю залишається ще недосконалим.

1.2. Кібербезпека в системі національної безпеки України

Стрімкий розвиток інформаційного суспільства складає інформаційно-комунікаційні технології (ІКТ), що обумовлюють виникнення питання щодо визначення сутнісних ознак кібербезпеки як компоненту інформаційної безпеки.

Для того щоб визначити ці сутнісні ознаки, потрібно розуміти зміст поняття інформаційної безпеки, яке наводиться в літературі, а також закріплено в нормативно-правових актах та допоможе зрозуміти загальну суть. Наведемо кілька основних понять:

1. Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

2. Інформаційна безпека – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень і дій, що приймаються.

3. В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [30].

Отже, можна констатувати, що інформаційна безпека – це стан захищеності важливих інтересів особи, суспільства і держави в інформаційній сфері від негативних інформаційних впливів в усіх сферах життєдіяльності , а також заподіяння шкоди через неповноту, недостовірність даних, негативні наслідки використання інформаційних технологій та забороненої для поширення інформації.

Виходячи з визначень поняття «інформаційна безпека», можна навести сутнісні ознаки:

− конфіденційність: стан інформації, при якому доступ до неї отримують тільки суб'єкти, які мають на це право;

− цілісність: запобігання несанкціонованій або незаконній модифікації інформації ;

− доступність: запобігання тимчасового або постійного приховування інформації від користувачів, які отримала право на доступ.

На даний час більшість загроз інформаційної безпеки реалізується шляхом несанкціонованого проникнення до сховищ інформації (комп'ютерів та серверів певних користувачів або організацій та установ).

Головні цілі таких атак:

− заміна достовірної інформації на недостовірну;

− викрадення конфіденційної інформації та подальше її нелегальне використання або вимагання за неї грошових еквівалентів;

− порушення стабільності роботи інфраструктури організацій та країни в цілому;

− внесення соціальної, політичної та економічної дестабілізації [10, 14-15 с.].

Для боротьби з цими атаками в політиці інформаційної безпеки на національному рівні реалізується державними органами влади та неурядовими організаціями. Урядові установи відповідають за розробку і координацію політики та захисту в сфері інформаційної безпеки. Здійснення державної політики належить до обов'язків структурних підрозділів міністерств, комп'ютерними групами швидкого реагування на інциденти в сфері інформаційної безпеки та установами з питань захисту даних [28, С.44].

Виходячи з цього, розглянемо, що включає в себе кібербезпека та які чинники впливають на протидію загрозам в інформаційній сфері. Отже, поняття кібербезпеки – це вже новий виток інформаційної безпеки, який спрямований саме на цифрове середовище, в якій власне знаходиться суспільство. Кібербезпека має на увазі не тільки сам захист інформації, а й захист всієї системи в інформаційному полі, в ІТ-полі в цілому.

Кібербезпека включає в себе захист інформації, але не обмежується лише нею. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити та вкрасти дані, але і вплинути на роботу, і продуктивність співробітників, використовувати інформацію проти людини або структури, а також зупинити виробництво. Кібербезпека сьогодні відповідає за три чинники: системи, процеси, люди [31].

З огляду на ці чинники сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту в рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у

кіберпросторі, розробленню та впровадженню ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі. Також потрібен перехід на міжнародні стандарти кібербезпеки, в тому числі галузеві. Найважливішим кроком є заміна науково-дослідних інститутів на більш ефективний та сучасний базовий стандарт та впровадження конкретних галузевих стандартів кібербезпеки [59, С.47].

Велику роль у сфері захисту інформації та кібербезпеки відіграє міжнародно-правове регулювання. Міжнародне співтовариство на різних рівнях прийняло ряд актів, що мають значення для захисту інформації та кібербезпеки, причому особливу роль відіграють регіональні акти, оскільки універсальний документ на даний час створити важко. Разом із тим не можна не відзначити спроби держав поширити норми глобальних міжнародних договорів на боротьбу з кіберзлочинністю або укласти нові договори. Наприклад, оскільки в кіберпросторі поряд з окремими особами можуть діяти й організовані злочинні групи, існує можливість застосування до них міжнародних договорів, спрямованих на боротьбу з організованою злочинністю, зокрема Конвенції ООН проти транснаціональної організованої злочинності від 15.11.2000 року [40, С.382].

На сьогоднішній день саме від захисту процесів, інформації та діяльності в кіберпросторі залежить дуже багато, ніж просто втрата інформації. Збереження системи, процесів, людського життя – всі ці складові намагається забезпечити кібербезпека для нормального функціонування життєдіяльності.

Отже, можна дійти такого висновку, кібербезпека є станом захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства та держави в інформаційній сфері. Одними з основних елементів кібербезпеки є: безпека інформації, даних, мережі, відновлення після кібератак, забезпечення кіберзахисту, операційна, хмарна, критична безпека інфраструктури, фізична безпека. З огляду на сучасні суспільно-політичні та

інформаційні чинники ефективність системи кіберзахисту є комплексном протидії кіберзагрозам, який сприятиме формуванню ефективного механізму безпеки у кібернетичній сфері. Кібербезпека є складовою частиною інформаційної безпеки, оскільки має ефективні засоби та інструменти можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі.

1.3. Нормативно-правове регулювання кібербезпеки України

Кібербезпека будь-якої сучасної держави має прямий вплив на всі складові частини її політики. Загрози, які виникають в кіберпросторі і впливають на державу це найбільші ризики, з якими може стикнутися будь-яка країна. Тому для запобігання таких ризиків щодо системи кібербезпеки потрібно дослідити формування законодавства, пріоритети та напрямки розвитку нормативно-правового регулювання у сфері кібербезпеки.

На сьогоднішній день 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. Не розв'язаними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури, триває розроблення підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки [8, С.106].

Першим етапом на шляху до створення законодавства про кібербезпеку стало прийняття Закону про основні принципи забезпечення кібербезпеки України в 2017 році. Аналізуючи даний нормативний акт, варто відмітити, що він носить скоріше декларативний характер та не передбачає ані вимог до систем безпеки, ані інструкцій на випадок атаки. Разом з цим Законом, який має досить

обмежену сферу дії, існує ряд інших підзаконних актів, які хоч і діють, але втратили свою актуальність [46]. Розглянемо, ці нормативно-правові акти, які становлять законодавчий характер.

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

Одним з основних нормативних актів є Стратегія кібербезпеки України, яка передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки, що засноване на напрацьованому за п'ять років гібридної війни досвіді, усвідомленні та імплементації досвіду та нормативних документів ЄС та НАТО [8, С. 102].

Формулюючи основні напрями державної політики щодо забезпечення кібербезпеки та інформаційної безпеки, внаслідок розділення цих сфер безпеки, не вдалося уникнути певного дуалізму і у формулюванні напрямів політики. Зокрема, створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них і моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації є багато у чому пов'язаними заходами. До того ж розвиток інформаційної інфраструктури держави стосується не тільки забезпечення кібербезпеки, а й інформаційної безпеки також [25, С. 107].

Отже, станом на 2019 рік закріплено таку законодавчу базу у сфері кібербезпеки держави: затверджено Доктрину інформаційної безпеки України (введена в дію 25.02.2017 р.), закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII (набрав чинності 09.05.2018 р.), «Про

національну безпеку України» 2469-VIII (набрав чинності 08.07.2018 р.), «Про інформацію» 2657-XII (редакція від 01.01.2017 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.), «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.) тощо. Декілька відповідних положень щодо кібербезпеки закріплена в указах президента, зокрема: «Про Концепцію розвитку сектора безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.); «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.), «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.) тощо [56, С.152].

З цього можна сформувати принципи на яких ґрунтується забезпечення кібербезпеки в Україні:

– 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 в 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. [8, С. 103].

Крім, законодавчих актів у сфері кібербезпеки є і нормативно-правові , такі як стандарти. Щодо питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій між вітчизняною професійною спільнотою і профільними державними органами. На даний момент в Україні в якості єдиного державного стандарту технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»[6, С.5].

Також, стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. При цьому кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [8, С.101].

Україна на даний час відчуває вплив кіберзлочиності, і об’єктивно зацікавлена в тому, щоб брати в цих дискусіях активну участь, оскільки міжнародний досвід у сфері правового забезпечення кібербезпеки та у сфері боротьби з кіберзагрозами є необхідним для неї як приклад у формуванні відповідної політики й побудови власної системи правового та організаційного забезпечення кібербезпеки. Створення дієвого механізму правового регулювання забезпечення та організації кібербезпеки в Україні є основним пріоритетом розвитку національної безпеки, яке потребує реорганізації та вдосконалення законодавчої бази, створення єдиної національної системи забезпечення кібербезпеки, організації та вдосконалення взаємодії суб’єктів

забезпечення кібербезпеки з провідними міжнародними інституціями [20, С.147].

В цілому забезпечення безпеки в кіберпросторі не тільки вичерпується заходами державного регулювання і контролю, а в багатьох випадках залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема суб'єктів господарювання. Наприклад, підвищений інтерес у кіберзлочинців викликає ринок криптовалют та електронної комерції. З допомогою різноманітних способів здійснення атак хакери здійснюють крадіжки електронних грошей безпосередньо у їхніх 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, наприклад, фішинг, який здійснюється за допомогою розсилки електронних повідомлень або використання шкідливого програмного забезпечення [8, С.105].

Виходячи з вище сказаного, можна зробити висновок, що на даний час кібербезпека тільки формує свою законодавчу базу, але протистояти загрозам потрібно уже зараз. Для цього існують відповідні органи, які відстежують спроби крадіжки, різних атак, які впливають на життєдіяльність суспільства. Отже, правове регулювання кібербезпеки в Україні здійснюється низкою законів та нормативно-правових актів, які в свою чергу забезпечують законність, доступність, захищеність кібепростору.

Висновки до розділу 1

Отже, підсумовуючи викладене у розділі 1 дослідження, можна зробити такі висновки:

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне

виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам. Захищеність інформаційних технологій супроводжується прийняттям та розробленням більшістю країн світу стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших) для нормального функціонування цифрових процесів. Тому кіберпезпека є найважливішим елементом у системі національної безпеки кожної держави, мета якої полягає у забезпеченні безпеки кібепростору.

Поняття інформаційна безпека ширше кібербезпеки і крім питань, пов'язаних з технічним забезпеченням безпеки інфраструктури та безпеки інформації, розглядає проблеми захисту особистості й суспільства від деструктивного інформаційного впливу. Кібербезпека є складовою частиною інформаційної безпеки. Кібербезпека важлива, оскільки урядові, військові, корпоративні, фінансові та медичні організації збирають, обробляють та зберігають безпрецедентні обсяги даних на комп'ютерах та інших пристроях. Значна частина цих даних може бути конфіденційною інформацією, будь то інтелектуальна власність, фінансові дані, особиста інформація або інші типи даних, для яких несанкціонований доступ або викриття можуть мати негативні наслідки. Організації передають конфіденційні дані через мережі та на інші пристрої в процесі ведення бізнесу.

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки. Проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає

скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства. Так, автоматизовані системи управління уможливлять використання технічних пристроїв замість робочої сили за небезпечних для життя людей обставин. Важливо змінити стереотип у суспільстві, що людина та її особисті дані нікому не цікаві, доцільно навчати фахівців користуватися захищеними протоколами передавання інформації, використовувати захищені інформаційні системи для роботи, а працівникам ІТ-сфери – обґрунтовувати необхідність застосування нових безпечних принципів роботи клієнтів в інформаційних системах.

Законодавчий рівень протидії загрозам є найважливішим для забезпечення захисту інформації в кіберпросторі. Розробка та прийняття законодавчих актів покликані створити умови для безпечного використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу та витоку технічними каналами. Також на законодавчому рівні має бути вирішено питання захисту громадян, суспільства і держави від неправдивої інформації, реалізації технічних та інших складових безпеки.

Інформаційні відносини, пов’язані із забезпеченням кібернетичної безпеки, вже врегульовані Законами України «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про охорону прав на промислові зразки», «Про авторські права та суміжні права», «Про державну підтримку засобів масової інформації та соціальному захисту журналістів», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в українських засобах масової інформації», «Про Національну програму інформатизації», «Про науково-технічну інформацію», «Про телекомунікації», «Про доступ до публічної інформації» та ін..

Отже, складова забезпечення кібербезпеки проявляється у створенні ієрархічної структури суб'єктів його реалізації, яких наділено владними повноваженнями. Правове регулювання є ключовою правовою засадою забезпечення кібербезпеки, так як проявляється у роботі великої кількості владних суб'єктів та процесі реалізації державної політики у сфері кібербезпеки.

РОЗДІЛ 2. КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНІЙ СФЕРІ

2.1.Кіберзлочини: поняття, види та класифікація

На сьогоднішній день використання інформаційних технологій не має меж. Цифровий простір переймає від реального все, що функціонує, в тому числі й злочинність у її нових формах та проявах. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша

особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні [33]. Отже, розглянемо, що ж означає термін «кіберзлочинність» і які категорії кіберзлочинів існують.

У міжнародній доктрині під поняттями кіберзлочини, кіберзлочинність охоплюються різні види правопорушень. У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 року по попередженню злочинності і поводженню з правопорушниками було зазначено, що існує дві категорії кіберзлочинів:

1) кіберзлочини у вузькому розумінні («комп'ютерні злочини»): будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних;

2) кіберзлочини в широкому розумінні («злочини, пов'язані з використанням комп'ютерів»): будь-яке протиправне діяння, яке вчиняється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [37, С. 44].

Звідси робимо висновок, що кіберзлочинністю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, з метою видозміни комп'ютерних даних. При цьому комп'ютер виступає в якості предмета злочину, а інформаційна безпека об'єкта. До подій, пов'язаних зі злочином можна віднести ситуації, при яких комп'ютер – знаряддя для вчинення злочинів, з метою порушення авторських прав, громадської безпеки, прав власності, моральності.

Розглянемо класифікацію кіберзлочинів для розуміння сутності загроз, які можуть виникнути:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

– незаконний доступ, наприклад, шляхом злому, обману та іншими

засобами;

– нелегальне перехоплення комп'ютерних даних;

– втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

– втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

– зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Також з урахуванням мотивації злочинців, кіберзлочини можуть бути умовно розділеними на наступні категорії: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини [49, 33 с.].

Одним з небезпечних кіберзлочинів на даний час є кібератака, яка безпосередньо впливає на певний об’єкт та має глобальні наслідки. Тому для того, щоб зрозуміти, чим вона небезпечна потрібно розглянути суть цього поняття. Відомий український дослідник з питань кібербезпеки В.Л. Бурячок

сформулював таке визначення поняття «кібератака» – це сукупність узгоджених щодо мети, змісту й часу дій або заходів, так званих кіберакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об’єкта [13].

Розглянемо, на які види поділяються кібератаки:

1) Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти») [33].

2) Фішинг – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів. Це схема, за допомогою якої шахраї, користуючись довірливістю або неуважністю людей, змушують їх самостійно розкривати особисту інформацію про себе для наступного її використання у зловмисних цілях [63].

3) Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

4) Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку [33].

5) Піратство – відтворення і розповсюдження мережею Інтернет фільмів, музичних творів, комп’ютерних програм, інших об’єктів інтелектуальної власності, без дозволу автора або іншої особи, яка має авторське право і суміжні права, або без виплати винагороди за використання творів у встановленому законом порядку. Вчинення будь-яких дій, які визнаються порушенням авторського права і суміжних прав з використанням мережі Інтернет [45].

6) Кардшаринг – надання незаконного доступу до перегляду супутникового та кабельного TV.

7) Соціальна інженерія – технологія управління людьми в Інтернет-просторі.

8) Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення.

9) Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

10) Рефайлінг – незаконна підміна телефонного трафіку [33].

11) SQL ін'єкція (англ. SQL injection) - один з найпоширеніших способів злому web-ресурсів, програм, які працюють з даними. Його мета - впровадити в запит сторонній, чужий SQL-код.

12) PHP ін'єкція – теж спосіб злому веб-сайтів, які написані на PHP. Основна думка - впровадження свого розробленого сценарію в код на серверній стороні ресурсу, що призводить до виконання сторонніх команд. Відомо - в багатьох розповсюджених движках та на форумах, які працюють на PHP (найчастіше це застарілі версії), є не зовсім продумані модулі та конструкції з уразливими місцями. Хакери шукають ці уразливості, аналізують їх, та користуються ними.

13) XSS (Cross Site Scripting, "міжсайтовий скриптинг") являє собою атаку, при якій зловмисник публікує на сайті, що атакується, скрипт, який виконується у користувачів при відкритті ними сторінок. Оскільки цей скрипт виконується в браузері у користувача, то він має доступ до інформації в його cookie, й може виробляти дії на сайті від імені користувача (якщо той "залогінився"), наприклад, писати, читати та видаляти повідомлення.

14) CSRF (англ. Cross Site Request Forgery - «міжсайтова підробка запиту», також відома як XSRF) - вид атак на відвідувачів веб-сайтів, який використовує недоліки протоколу HTTP.Коли користувач заходить на сайт, який створив зловмисник, від користувача таємно відправляється запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Для здійснення

даної атаки жертва повинна бути автентифікована на тому сервері, на який відправляється запит, і цей запит не повинен вимагати будь-якого підтвердження з боку користувача,яке не може бути проігноровано або підроблено атакуючим скриптом [21, С.131-133].

Отже, до кіберзлочинів належить будь-який злочин, вчинений із застосуванням електронних способів та засобів. Поняття "кіберзлочин" не обмежується тільки рамками Інтернету, воно поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері. Існує велика класифікація кіберзлочинів, але одним із небезпечних видів є кібератака. Вона спрямовується як сукупність узгоджених заходів, які можуть зашкодити нормальному функціонуванню всіх сфер життя. Є багато видів кібератак, які розповсюджуються у віртуальному середовищі та в мережі Інтернет.

2.2. Кіберправопорушники: типи та характеристики

На даний момент людство переживає бурхливий розвиток автоматизації, інформатизації та комп'ютеризації всіх сфер життя. Це надає нові можливості для розвитку національної культури, освіти, науки й економіки. Але поширення інформаційних технологій має й негативний аспект: відкриває шлях до злочинної поведінки. Комп'ютерні системи надають нові, дуже досконалі можливості для невідомих раніше правопорушень, а також для скоєння традиційних злочинів, але нетрадиційними засобами.

Застосовуючи метод типології, спробуємо поділити всю сукупність вітчизняних кіберправопорушників на окремі, найбільш характерні та узагальнені типи, враховуючи при цьому високий рівень латентності даного різновиду злочинності та неможливість його об'єктивного відображення у статистичних даних. Можна виділити шість типів кіберзлочинців, які поширені в українському суспільстві:

1) Хакери - власне фахівці у сфері інформаційних технологій, які

використовують власні навички для протиправних дій.

2) Кіберзлочинці, які, наприклад, вчиняють кібератаки на об’єкти критичної інфраструктури. Даний вид правопорушень може керуватися й благородною метою (наприклад, хактивізм), бути альтруїстичним та некерованим ззовні, виявлятися як форма протесту, зумовленого намаганням офіційних структур контролювати Інтернет, а неформальних структур – зберегти конфіденційність та анонімність.

3) Особи та групи, які потрапляють в поле зору традиційної та організованої злочинності, і зрештою, кіберзлочинність перетворюється на один із напрямків у протиправній діяльності організованого та традиційного криміналу. На даний час зафіксовано достатньо фактів того, що кіберзлочини вчиняються кримінальниками, в тому числі й із установ виконання покарань, наприклад, шляхом телефонного шахрайства з місць позбавлення волі.

4) «Білокомірцеві» злочинці, які використовують кіберсферу для вчинення злочинів в економічній, фінансовій тощо сферах.

5) Пересічні громадяни країни, які порушують авторські права. Використання піратського програмного забезпечення зберігається як масове явище в українському суспільстві.

6) Пересічні громадяни, які вчиняють інші, крім піратства, правопорушення із застосуванням технічних приладів та віртуальної мережі[60, С. 85-86].

Зупинимось на першому типі кіберправопорушників, оскільки поняття «хакер» не є тотожним поняттю «кіберзлочинець», потрібно зрозуміти сутність поняття.

Хакер - надзвичайно кваліфікований ІТ -спеціаліст, людина, яка розуміє самі основи роботи комп'ютерних систем. Спочатку хакерами називали програмістів, які виправляли помилки в програмному забезпеченні яких-небудь швидким і далеко не завжди елегантним (в контексті використовуються у програмі стилю програмування та її загальної структури, дизайну інтерфейсів)

або професійним способом; такі правки асоціювалися з «грубої роботою» через за їх грубості, звідси і пішла назва «хакер»[58].

Існують багато різних типів хакерів, які мають добрі наміри та злі цілі. Розглянемо, основні типи хакерів.

Хакер мережевий - займається дослідженням програмного забезпечення, встановленого на Internet - серверах (або в локальних мережах), з метою отримання несанкціонованого доступу до сервера або порушення його роботи-так звані DoS (Denial of Service) атаки.

Кракер (cracker) - займається зломом прикладного програмного забезпечення, зазвичай для того, щоб отримати програми з обмеженою функціональністю, призначених, в основному, для демонстрації користувачеві можливостей повної версії.

Фрікер (phreaker) - досліджує телефонні мережі з метою знайти можливість дзвонити безкоштовно. Історично фрикерство-найперший вид хакерської діяльності, що виник ще в 60-70-ті роки XX століття. В останні роки фрикери стали займатися також і дослідженням мереж для мобільних телефонів.

Кардер (carder) - займається нелегальним отриманням номерів кредитних карт і відомостей про їх власників. Часто ця діяльність поєднується з хакерською. Кардерство вважається найбільш серйозним злочином, і тому є найнебезпечнішим видом хакерської діяльності [15].

Білий капелюх - цей тип хакера використовує свої зловмисні здібності за добру справу. Наприклад тестування безпеки та перевірка того, як система захисту на комп'ютері повідомляє власника про наявність прогалин.

Чорна шапочка - цей тип хакера є протилежною шапці білого,чорний капелюх використовує можливості злому для вчинення злочинів, таких як примушування до безпеки системи для крадіжки наявних даних і використовується для речей, які не є хорошими.

Сірий капелюх - називається сірим, оскільки цей тип хакерів використовує свою науку про хакерство для добра і зла.

Хактивіс мотивований особистими думками з питань політики, релігії, навколишнього середовища тощо.

Сценарій малюка- цей тип хакера використовує справжнє програмне забезпечення, яке змінило сценарій для входу в систему [55].

Кібертерористи – це кіберзлочинці, які роблять 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 [24, С.63].

На сьогоднішній день кібертероризм є одним із найнебезпечніших видів злочинності, який спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, пригнічення засобів мережевого інформаційного обміну і здійснення інших деструктивних дій. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж, і в проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність через підставні комп'ютери, що ускладнює його ідентифікацію та визначення місцезнаходження[64, С. 58].

Таким чином, кіберправопорушення у кіберпросторі є доволі поширеним соціальним явищем не лише у світі, а й в українському суспільстві, яке має високу динаміку зростання та латентність. Водночас природа цих правопорушень, а відтак і типів кіберзлочинців, які їх уособлюють, є різною. Кожен із типів кіберправопорушників має свою мотивацію до вчинення злочинів у кіберсфері. Здійснюючи певні атаки у цифровому середовищі кіберзлочинці завдають значної шкоди на локальному, державному та міжнародному рівні.

2.3.Особливості запобігання кіберзлочинів в Україні

Цифрове середовище займає важливе місце в повсякденному житті

суспільства. Існує чимало можливостей, які виникають в мережі Інтернет: щоденне спілкування, пошук потрібної інформації, здійснення покупок, банківських операцій тощо. Проте з цим постає необхідність в створенні ефективного механізму захисту персональних даних в мережі Інтернет. Розширення цієї сфери надає можливості вивчення традиційних злочинів і створює умови для реалізації принципово нових схем і методів злочинної діяльності.

Найбільшим розповсюдженням злочинності є мережа Інтернет, в якій відсутні механізми контролю, необхідні для правозастосування. Мережа Інтернет створювалася технологічно як структура без ієрархії та без якогось "ядра", зруйнувавши які можна було б паралізувати її роботу, і навряд чи хтось міг уявити масштаби розвитку проекту, спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, і важко було передбачити подальший масштаб її розвитку, її економічну та соціальну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини вкупі з її доступністю й легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі та відсутність національних кордонів у кіберпросторі зумовили можливості для росту злочинності та на роки відклали розроблення механізмів правового та соціального контролю у сфері використання інформаційних мереж для вчинення злочинів. Атаки в мережі, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, корпоративне шпигунство та поширення дитячої порнографії – ось тільки деякі зі злочинів, що вчиняються в мережі Internet [7, С.17].

Для того щоб запобігти кіберзлочинності, доцільно розглянути деякі заходи протидії злочинів, об'єднавши їх в три групи: технічні, організаційні, правові.

Технічні заходи захисту від несанкціонованого доступу до комп'ютерних

систем передбачають:

– використання засобів фізичного захисту, включаючи засоби захисту кабельної системи або електроживлення, засоби архівації та копіювання інформації на зовнішні носії;

– організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок;

– розробку програмних засобів захисту, в тому числі антивірусних програм, систем;

– розмежування повноважень, програмних засобів контролю доступу;

– прийняття конструктивних заходів захисту від розкрадань і диверсій;

– установку резервних систем електроживлення;

– оснащення приміщень замками, установку сигналізації і багато іншого.

До організаційних заходів можна віднести:

– ретельний підбір персоналу;

– виключення випадків ведення особливо важливих робіт лише однією особою;

– шифрування даних для забезпечення конфіденційності інформації;

– заходи захисту, що включають контроль доступу в приміщення, розробку стратегії безпеки, планів дій у надзвичайних ситуаціях і т. ін.;

– організація надійної та ефективної системи архівації і дублювання найбільш цінних даних;

– захист інформації від несанкціонованого доступу, включаючи використання різних пристроїв для ідентифікації особи за біометричною інформацією - райдужній оболонці ока, відбитками пальців, голосу, розмірами кисті руки;

– покладання персональної відповідальності на конкретних осіб, покликаних забезпечити безпеку об’єкта, введення в штат фахівців у галузі безпеки інформації;

– забезпечення універсальності засобів захисту від усіх користувачів; розробка плану відновлення працездатності об’єкта після виходу його з ладу і т. п.

До правових заходів належать:

– посилення норм, що встановлюють відповідальність за комп'ютерні злочини;

– захист авторських прав програмістів;

– вдосконалення кримінального та цивільного законодавства в цій сфері.

Також належать питання громадського контролю за розробниками комп'ютерних систем і прийняття міжнародних договорів про обмеження у їх діяльності [54, С. 56-57].

На жаль, в Україні боротьба з кіберзлочинністю перебуває на початковому етапі впровадження інституцій та механізмів у сфері кібербезпеки, проте певну законодавчу базу вже створено – необхідно лише її дотримуватися та розвивати.

Варто сподіватись, що наша державна влада не зупиниться на досягнутому, буде запозичувати досвід інших країн Європи та США і брати участь у міжнародній співпраці з питань кібербезпеки.

Але не варто забувати про власну інформаційну безпеку, і тому слід дотримуватися декількох основних правил:

- користуватися ліцензійним програмним забезпеченням;
- не повідомляти стороннім особам персональні дані, дані та паролі доступу до банківських карток і систем;
- не завантажувати та не відкривати підозрілі комп'ютерні файли;
- перевіряти інформацію, особливо банківську, лише з офіційних сайтів або за офіційними номерами телефонного зв'язку;
- не відвідувати та не вводити персональні дані на підозрілих сайтах;
- не довіряти повідомленням у месенджерах або смс про виграші та акції сумнівного походження;

– користуватися антивірусом;

– використовувати складні, неоднакові паролі та не зберігати їх на телефоні або комп'ютері;

– не зберігати інформацію «небажаного» характеру на телефонах і комп'ютерах [32];

– не завантажувати програмне забезпечення з ненадійних джерел;

– створювати складні паролі;

– не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;

– намагатися користуватися двофакторною аутентифікацією;

– не переходити на підозрілі посилання та за спливаючими вікнами;

– не заходити на ненадійні сайти та не завантажувати з них жодних програмних забезпечень;

– не вставляти у свій комп’ютер флешки та зовнішні диски, якщо не довіряєте повністю їх джерелу;

– періодично здійснювати резервне копіювання важливої інформації;

– тримати свої гаджети в полі зору, коли знаходитися у місцях, де до них може бути доступ сторонніх осіб.

Виконання зазначених засобів безпеки дозволить лише мінімізувати можливість випадкового несанкціонованого проникнення у ваші пристрої та системи. Однак неможливо надати повної гарантії уникнення зламу. Для максимальної мінімізації таких ризиків компаніям рекомендовано користуватися послугами спеціалістів у сфері кібербезпеки з чітким виконанням всіх інструкцій, які вони зазначають [42].

Отже, підсумовуючи можна стверджувати, що в епоху стрімкого й активного розвитку інформаційних технологій кіберзлочини стають невід'ємною частиною нашого повсякденного життя, робочих процесів і діяльності державних органів та бізнесу, а тому особливу увагу слід приділяти власній кібербезпеці. На сьогоднішній день особливо важливо переглянути всі існуючі

заходи та активно розробляти нові, що принесуть більшу користь і надійніший захист від кіберзлочинців. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

Висновки до 2 розділу

Виходячи з вище викладеного у розділі 2 дослідження, можна зробити такі висновки, що кіберзлочинність – це незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей. З-поміж основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через Інтернет.

У інтернет-мережі зараз маса інформації щодо різних видів хакерських атак на web-сайти.

Злочинність як мінливе соціально негативне явище, яке супроводжує людство протягом усієї історії його існування, в епоху інформаційних технологій набуває нових форм та ознак. Інформаційні технології проникають та швидко опановують різноманітні сфери суспільства, в тому числі і сфери, які пов’язані з отриманням прибутків, наприклад, сферу економіки, фінансів, торгівлі, або сфери, які пов’язані із суспільною та національною безпекою, приватністю особистості тощо. Дані сфери переносяться у віртуальний світ, а відтак стають вразливими для кіберзлочинців. Отже, з поширенням інформаційних технологій кіберзлочинність перетворюється на віртуальну проблему як усього людства та створених ним інституцій, так і окремих індивідів. Відтак і протидія кіберзлочинності потребує нових підходів та рішень.

Водночас природа цих правопорушень, а відтак і типів кіберзлочинців, які їх уособлюють, є різною. Кожен із типів кіберправопорушників має свою мотивацію до вчинення злочинів у кіберсфері. Одним найбільш поширеними

видом кріберзлочинців є хакери. Хакери мають багато можливостей, щоб скористатися вразливістю кібербезпеки та досягти своїх злочинних цілей. Сьогодні можна виділити такі основні (найпопулярніші) способи:вішинг, фішинг, кардинг, соціальна інженерія, вірус, злом, кібератака, кібертероризм тощо. Найбільш небезпечними видами кіберзлочинності є кібератаки та кібертероризм. Сьогодні кількість кібератак і прикладів кібертероризму дедалі зростає, а рівень шкоди суттєво збільшується. Найбільшу проблему становить відсутність чіткого законодавства, в якому було б чітко визначено це поняття, передбачено відповідальність за протиправні діяння, що свідчить про недостатнє осмислення цього явища. Труднощі у визначенні поняття «кібертероризм» пов'язані переважно з тим, що складно відокремити сам кібертероризм від акцій інформаційної війни й застосування інформаційної зброї, від злочинів у сфері комп'ютерної інформації або патріотичних поривів населення країн і регіонів. Додаткові труднощі виникають у разі спроби виявити специфіку цієї форми тероризму. Так, наприклад, психологічний та економічний аспекти кібертероризму тісно переплетені, і неможливо однозначно визначити, який із них має більше значення.

Для того щоб захиститися від кіберзлочинів потрібно вживати заходи щодо протидії цим злочинам. До числа основних заходів протидії комп'ютерній злочинності можна віднести:

– створення єдиної стратегії боротьби з кіберзлочинністю відповідно до якої функції силових відомств чітко розподілені і координуються державою;

– створення загального центру для моніторингу загроз кібертероризму і розробки заходів швидкого реагування;

– організацію якісного захисту матеріально-технічних об'єктів, що складають фізичну основу інформаційної інфраструктури, насамперед критичної;

– розвиток технологій виявлення впливів на інформацію та її захисту від

несанкціонованого доступу, спотворення чи знищення;

– безперервну підготовку персоналу інформаційних систем до ефективного протистояння різним варіантам дій терористів;

– розвиток міждержавного співробітництва у боротьбі з кіберзлочинністю.

Але варто також пам’ятати про свою власну комп’ютерну безпеку. Тому потрібно дотримуватись деяких порад:

– користуватися ліцензійним програмним забезпеченням;

– не повідомляти стороннім особам персональні дані, дані та паролі доступу до банківських карток і систем;

– не завантажувати та не відкривати підозрілі комп'ютерні файли;

– перевіряти інформацію, особливо банківську, лише з офіційних сайтів або за офіційними номерами телефонного зв'язку;

– не відвідувати та не вводити персональні дані на підозрілих сайтах;

– не довіряти повідомленням у месенджерах або смс про виграші та акції сумнівного походження;

– користуватися антивірусом;

– використовувати складні, неоднакові паролі та не зберігати їх на телефоні або комп'ютері;

– не зберігати інформацію «небажаного» характеру на телефонах і комп'ютерах; тощо.

– не завантажувати програмне забезпечення з ненадійних джерел;

– створювати складні паролі;

– не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;

– намагатися користуватися двофакторною аутентифікацією;

– не переходити на підозрілі посилання та за спливаючими вікнами;

– не заходити на ненадійні сайти та не завантажувати з них жодних програмних забезпечень;

– не вставляти у свій комп'ютер флешки та зовнішні диски, якщо не довіряєте повністю їх джерелу;

– періодично здійснювати резервне копіювання важливої інформації;

– тримати свої гаджети в полі зору, коли знаходитися у місцях, де до них може бути доступ сторонніх осіб.

Отже, підсумовуючи можна стверджувати, що правопорушення у кіберсфері є доволі поширеним соціальним явищем не лише у світі, а й в українському суспільстві, яке має високу динаміку зростання та латентність. Якщо профілактика та протидія одним правопорушенням потребує інформаційної та роз'яснювальної роботи або лежить у площині зростання рівня економічного добробуту населення, то профілактика та протидія іншим кіберзлочинам полягає в поширенні знань про кібербезпеку починаючи зі шкільного віку, посиленні кримінальної відповідальності на законодавчому рівні, залученні до кібербезпеки комп'ютерних інтелектуалів тощо. Відтак профілактика та протидія даним правопорушенням потребують різних підходів в залежності від окремого типу кіберзлочінців.

РОЗДІЛ 3. СТРАТЕГІЧНИЙ РОЗВИТОК КІБЕРБЕЗПЕКИ В УКРАЇНИ: ЦІЛІ , ЗАВДАННЯ ТА ПРІОРІТЕТИ

3.1. Стратегічні цілі формування національної системи кібербезпеки України

Одним із головних законодавчих актів у сфері регулювання кібербезпеки України є «Стратегія розвитку кібербезпеки України» (далі – Стратегія), яка була прийнята в 2016 році. Це була перша спроба стратегування державної політики щодо сфери кібербезпеки. Документ формувався на фоні агресії РФ проти України, першого в Україні випадку кібератаки проти об'єкта критичної інфраструктури (ОКІ) енергетичного сектору, а також загального зростання деструктивної кіберактивності [26, С.1].

За ці роки було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який є правовим підґрунтям для створення національної системи кібербезпеки та виконання її основними суб'єктами завдань у сфері кібербезпеки.

Отриманий протягом часу дії Стратегії досвід надав змогу виокремити низку системних проблем, які або ускладнювали, або унеможливлювали її ефективну реалізацію. Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Не були розроблені індикатори виконання Стратегії, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань. Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились

епізодично. Нова Стратегія кібербезпеки України враховує цей досвід і проблеми та визначає механізми реалізації Стратегії на наступний п'ятирічний період[47, С.3-5].

14 травня 2021 року набрав чинності Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 26 серпня 2021 р. № 447/2021. Відповідно до затвердженої Стратегії Україна створюватиме максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави.

Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним визнано:

– посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

– набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

– забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме Національний координаційний центр кібербезпеки [43]. Він здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і

оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення «Стратегії кібербезпеки України» [34].

Зважаючи на вище вказане, зміст нової редакції «Стратегії кібербезпеки України (2021-2025 роки)» сформований наступним чином:

Розділ 1. Кібербезпека: глобальний контекст. Визначає шляхи посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Розділ 2. Стан реалізації Стратегії кібербезпеки України на 2016-2020 роки. Показує сильні та слабкі сторони Стратегії 2016 року, яка дала поштовх у запровадженні підходів довгострокового планування в цій сфері, а отже, сам факт її прийняття є позитивним результатом.

Розділ 3. Національна система кібербезпеки: засади розбудови. Визначає шляхи розбудови Національної системи кібербезпеки, які дадуть можливість розширити запропоновані дії на всі галузі економіки та сфери діяльності.

Розділ 4. Національний кіберпростір: виклики та кіберзагрози. Формує основні виклики у сфері кібребезпеки: упровадження нових технологій, цифрових послуг та механізмів взаємодії громадян з державою, включаючи виборчий процес, створює велику кількість прихованих взаємозв’язків на рівні технологій і процесів.

Розділ 5. Пріоритети забезпечення кібербезпеки України та стратегічні цілі. Визначає пріоритети забезпечення кібербезпеки України, які потребують чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії.

Розділ 6. Стратегічні завдання. Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Розділ 7. Напрямки зовнішньополітичної діяльності України у сфері кібербезпеки. Визначає зовнішньополітичні напрями у сфері кібербезпеки, які є

поглибленням євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Розділ 8. Механізми реалізації Стратегії та забезпечення відкритості. Формує основні критерії результативності Стратегії з досягненням мети та стратегічних цілей шляхом виконання визначених стратегічних завдань.

Розділ 9. Виміри успіху (метрики). Показує ефективність реалізації Стратегії та індикатори, які мають визначають прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації завдань Стратегії [47, С. 1-27].

Стратегія передбачає:

– захист критичної інфраструктури, який має передбачати, зокрема, комплексне вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, визначення критерії в віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;

– формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;

– розроблення та запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі, налагодженню співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури;

– формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

– залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у цій сфері;

– підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі;

– розвиток міжнародного співробітництва та підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України з ЄС та НАТО [48, С. 9].

Значення кіберпростору в розвитку цивілізації повсякчас зростає і поступово перетворюється на одну зі сфер міждержавного протиборства. Прогнозування розвитку безпекового середовища навколо України на період до 2025 року демонструє, що суб'єктам забезпечення національної безпеки держави необхідно терміново вжити запобіжних заходів для захисту національних інтересів в інформаційному просторі, невід'ємною частиною якого є кіберпростір[44].

Стратегія кібербезпеки України 2021-2025 «Безпечний кіберпростір – запорука успішного розвитку країни» розроблена з урахуванням аналізу виконання Стратегії кібербезпеки України (2016-2020 роки), результатів соціологічних опитувань та емпіричних досліджень, а також досвіду найкращих європейських практик.

Мета створення Стратегії: документ має стати якісним вказівником із довгостроковим плануванням та встановленням чітких критеріїв реалізації завдань. Він враховує конструктивні рекомендації експертів, світові тенденції, розвиток нормативно-правової бази для вирішення нагальних проблем у сфері кібербезпеки, створення умов для безпекового функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Ключовими засадами Стратегії є стримування, кіберстійкість, взаємодія [52, С.2].

Отже, розглянемо ці ключові засади, які включають в себе досягення певних стратегічних цілей. Для формування потенціалу взято орієнтир на досягнення таких стратегічних цілей:

– ціль С.1. Дієва кібероборона;

– ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму;

– ціль С.3. Ефективна протидія кіберзлочинності;

– ціль С.4. Розвиток асиметричних інструментів стримування.

Для набуття кіберстійкості (К) необхідним є досягнення таких стратегічних цілей:

– ціль К.1. Національна кіберготовність та надійний кіберзахист;

–ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки;

– ціль К.3. Безпечні цифрові послуги.

Для вдосконалення взаємодії (В) необхідним є досягнення таких стратегічних цілей:

– ціль В.1. Зміцнення системи координації;

– ціль В.2. Формування нової моделі відносин у сфері кібербезпеки;

– ціль В.3. Прагматичне міжнародне співробітництво[43].

Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Стратегічними завданнями Стратегії є :

– запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

– забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів та оглядів у сфері кібербезпеки;

– запровадження у систему військово-патріотичного виховання та систему територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки;

– удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів;

– забезпечення максимального охоплення об'єктів критичної інфраструктури негласною перевіркою стану їх готовності до можливих кібератак та кіберінцидентів з метою превентивного усунення передумов до реалізації кіберзагроз;

– забезпечення постійного моніторингу розвитку кіберспроможностей міжнародних терористичних угруповань, спрямованого на своєчасне виявлення і нейтралізацію реальних та потенційних загроз скоєння на території України актів кібертероризму;

– розроблення методики збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах;

– врегульовання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів із стримування деструктивної діяльності в кіберпросторі;

– розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

Стратегічними завданнями на засадах кіберстійкості, визначено:

– розроблено базові вимоги та рекомендації з питань забезпечення кібербезпеки та кіберзахисту;

– розгорнення системи обміну інформацією про кіберінциденти між усіма суб'єктами забезпечення кібербезпеки;

– розроблено Загальнонаціональну програму кібергігієни, спрямовану на підвищення рівня кіберграмотності населення України;

– утворено центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері;

– впроваджено цифрові послуги для населення та розвиватиме національну інформаційну інфраструктуру, передбачаючи виділення коштів на заходи кібербезпеки та кіберзахисту в розмірі не менше ніж 5% від загальної вартості відповідного об’єкта інформаційної інфраструктури (інформаційно-комунікаційної системи);

– розроблено нові національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів;

Стратегічними завданнями на засадах взаємодії є:

– запровадження обов'язкового надання в режимі реального часу інформації про кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки або кіберзахисту до Національного координаційного центру кібербезпеки;

– розроблення та запровадження механізмів заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки держави;

– врегулювання на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проєктів у цій сфері;

– запровадження на регулярній основі проведення консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічно сприятиме їх розвитку;

– створення постійно діючої робочої групи з питань взаємодії із провідними ІТ-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України;

– визначення та затвердження переліку пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України[47, 13-24 с.].

Зважаючи на досвід розвинених країн, згадані стратегічні цілі слід досягати через стратегічні функції діяльності національної системи забезпечення кібербезпеки держави, а саме:

– запобігання — заходи з завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

– захисту — заходи з забезпечення випереджувального захисту (в першу чергу кіберзахисту) від можливих кібератак (кібервпливу);

– запобігання та мінімізація загроз — заходи з безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) в разі безпосередньої загрози проведення кібератак. За певних умов в межах зазначеного можуть вживатися завчасні (зустрічні) заходи активного кіберзахисту;

– реагування — заходи комплексного реагування на факти загрози (кібератаки тощо) з боку супротивника та відповідне виконання суб’єктами забезпечення кібербезпеки держави впливу на супротивника, у т. ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з

одночасним вжиттям заходів з захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

– відновлення — заходи, спрямовані на відновлення інформаційної та іншої інфраструктури, які стали об’єктом кібератак, стабілізацію ситуації та ліквідацію інших негативних наслідків [44].

Ця Стратегія закладає загальну архітектуру національної системи кібербезпеки та розподіляє завдання та повноваження між основними суб’єктами забезпечення кібербезпеки (Радою національної безпеки і оборони, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв’язку та захисту інформації , Службою безпеки, Національною поліцією, Національним банком, розвідувальними органами України), передбачає створення умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та є власниками (розпорядниками) об’єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об’єднань і громадян. Запланований розвиток мережі команд реагування на комп’ютерні надзвичайні події, створення та забезпечення функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади; розбудова захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів [48, с. 9].

Підсумовуючи, можна стверджувати, що за сучасних умов в Україні, як і в інших країнах світу, при створенні нових інформаційних технологій, у результаті інтелектуальної діяльності виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що характеризуються національним значенням. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо. На цей час інформація стала

першоосновою життя сучасного суспільства, предметом та продуктом його діяльності, а процес створення, накопичення, збереження, передачі та обробки інформації, у свою чергу, стимулює прогрес в інформаційній сфері, у тому числі електронно-обчислювальну техніку, засоби телекомунікації та системи зв'язку.

Таким чином, з новими інформаційними досягненнями, державні кордони практично стають прозорими для обігу інформації. При цьому, чим більше зазначена сфера залучається в комерційний обіг, тим більше виникає потреба у захисті інтересів власників інформаційних об'єктів та їх користувачів, тобто забезпеченні інформаційного правопорядку [17].

3.2. Пріорітети забезпечення кібербезпеки України

Значення кіберпростору в розвитку цивілізації повсякчас зростає і поступово перетворюється на одну зі сфер міждержавного протиборства. Прогнозування розвитку безпекового середовища навколо України на період до 2025 року демонструє, що суб’єктам забезпечення національної безпеки держави необхідно терміново вжити запобіжних заходів для захисту національних інтересів в інформаційному просторі, невід’ємною частиною якого є кіберпростір [44].

Стратегія кібербезпеки України 2021-2025 «Безпечний кіберпростір – запорука успішного розвитку країни» розроблена з урахуванням аналізу виконання Стратегії кібербезпеки України (2016-2020 роки), результатів соціологічних опитувань та емпіричних досліджень, а також досвіду найкращих європейських практик.

Забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [53].

Концептуальні методологічні підходи до подальшого розвитку й удосконалення національної системи кібербезпеки базуються на таких пріоритетах:

– всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України;

– перманентності заходів з удосконалення законодавства у сфері кібербезпеки;

– орієнтованості на економічне і соціальне зростання суспільства; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту;

– визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності;

– ризик-орієнтованому підході щодо заходів забезпечення кібербезпеки та кіберзахисту;

– запровадженні механізмів державно-приватного партнерства у сфері кібербезпеки;

– проактивному підході, що передбачає здійснення випереджувальних заходів;

– забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки [19,С.118].

Основними пріоритетами забезпечення кібербезпеки України є:

– убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

– захист прав, свобод і законних інтересів громадян України у кіберпросторі;

– європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей:

– дотримання європейського підходу до забезпечення кібербезпеки як до спільної відповідальності усіх ключових стейкхолдерів;

– орієнтація на стандарти ЄС та НАТО в сфері забезпечення кібербезпеки замість застосування пострадянських або виключно радянських стандартів;

– відмова від пріоритету "захисту національного сегменту Інтернету", який є притаманним російському та китайському підходам до кібербезпеки [48, С. 8.].

Також важливим при формуванні формування стратегічних напрямків розвитку кібербезпеки є врахування останніх стратегічних напрацювань Європейського Союзу, інтеграція до якого є одним ключових завданнь зовнішньої та внутрішньої політики України. Таке врахування може відбуватись на декількох рівнях, що включає як оцінку безпекового середовища в якому формуються нові стратегічні пріоритети, так і самих пріоритетів. Європейський Союзу у грудні 2020 року оприлюднив свою нову Стратегію кібербезпеки, що дає розуміння викликів з якими стикається як сам Союз, так і його члени та до яких заходів він планує вдаватись щоб зробити європейський цифровий простір безпечнішим для громадян та бізнесу [26, С. 2].

З огляду на зазначене, головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. Україна співпрацюватиме з міжнародними партнерами, організаціями та іншими заінтересованими сторонами, які поділяють наше спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного та безпечного, в основі якого дотримання прав людини, основних свобод та демократичних цінностей, що є запорукою

соціально-економічного та політичного розвитку України. Ураховуючи взаємопов'язаність сучасного віртуального простору та з метою розвитку співпраці між державою, приватним сектором економіки, науковими і освітніми колами та громадянським суспільством у сфері кібербезпеки, Україна розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний і, насамперед, безпечний, що є запорукою успішного розвитку країни.

Кібербезпека України має стати одним з основних питань міжнародної діяльності країни, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал. З цією метою Україна має розвивати мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва[47, С.24].

Реалізація стратегічних напрямків розвитку кіберзпеки безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їхньої компетенції. Стратегія розвитку кібербезпеки в Україні ґрунтується на положеннях Конституції України, законів України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України», «Конвенції про захист прав людини і основоположних свобод», «Конвенції про кіберзлочинність», «Стратегії національної безпеки України», «Концепції боротьби з тероризмом в Україні» та інших нормативно-правових актів.

Таким чином, держава повинна гарантувати безпечне користування кіберпростором, отримуючи досвід та практики країн Європейського союзу, для подальшої їх реалізації.

Висновки до 3 розділу

Підсумовуючи, вище викладене в 3 розділі дослідження, можна стверджувати, що стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

14 травня 2021 року Ради національної безпеки і оборони України схвалила проєкт Стратегії кібербезпеки України на 2021-2025 роки. Основою для розробки документа стала Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року №392. Також було вивчено концептуальні положення стратегій із кібербезпеки країн ЄС, США, Японії, низку соціологічних опитувань й емпіричних досліджень, які було проведено наприкінці минулого і на початку 2021 року.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідними є:

– створення національної системи кібербезпеки;

– посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

– забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна

інфраструктура).

У Стратегії визначені основні виклики та загрози для України у сфері кібербезпеки. Основні виклики для України у сфері кібербезпеки:

– активне використання кіберзасобів у міжнародній конкуренції;

– змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;

– мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

– вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

– упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Паралельно з ухваленням Стратегії було створено Національний координаційний центр кібербезпеки як робочий орган РНБОУ.

Стратегічні цілі ґрунтуються на стримуванні, кіберстійкості, взаємодії.

Пріоритетами забезпечення кібербезпеки України є:

– убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

– захист прав, свобод і законних інтересів громадян України у кіберпросторі;

– європейська і євроатлантична інтеграція у сфері кібербезпеки.

Отже, ухвалення Стратегії є дуже важливим кроком в розбудові системи національної кібербезпеки, вкрай необхідним, але недостатнім, адже Стратегія не пропонує відповідної термінології та не передбачає внесення змін до чинних нормативно-правових актів. Ці питання планувалось врегулювати під час написання Закону України про кібербезпеку, який мав розроблятись саме так, як розроблялась Стратегія кібербезпеки.

ВИСНОВКИ

Отже, виходячи з поставлених для наукової проблеми завдань можна зробити, такі загальні висновки:

1. На даний час одним з фундаментальних наслідків глобальної інформатизації стало виникнення принципово нового середовища – кіберпростору. Використання Інтернету та інформаційних технологій не тільки відкриває перед людством безмежні можливості, а й створює нові серйозні

загрози. З цих причин і виникає потреба в кібербезпеці, яка дасть можливість для надійного захисту інформації в комп'ютерних мережах та системах. В сучасних умовах питання кібербезпеки виходять з рівня захисту інформації на окремому об'єкті та рівні створення єдиної системи кібербезпеки держави як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації у вузькому сенсі цього слова, а й усього кіберпростору.

Таким чином, питання щодо забезпечення кібербезпеки не втратить свою актуальність, оскільки відбувається стрімкий розвиток інформаційних технологій, що супроводжують виникненню нових загроз.

Сфера кіберпростору поширена у всьому світі завдяки виникненню цифрових та інформаційно-телекомунікаційних технологій. Це дало підставу до необхідності розв'язання проблем для запобігання сукупностей загроз. З цим і виникає поняття «кібербезпека», яке з'явилося в середині 1990-х років та досліджувалось у наукових працях різних вчених (В.А. Ліпкана, О.А. Баранова, О.Ю. Запорожець, В.Л. Бурячок та інших). Велика кількість країн досліджували різноманітні аспекти кібербезпеки розробляючи відповідні стратегії. Серед таких країн були США, Німеччина, Франція, Канада, Турецька Республіка, Нідерланди, Австралія, Україна та інші. Ці стратегії надавали різні визначення терміну «кібербезпека», тому узагальнюючи можна, сформувати, таке визначення поняття: кібербезпека – це інформаційна безпека в умовах використання цифрових систем та телекомунікаційних мереж, сукупуність заходів щодо запобігання шкоди, несанкціонованого доступу, кіберзагрозам та деструктивних атак, з метою забезпечення надійності, конфіденційності та захисту інформації для всіх сфер життєдіяльності.

2. Кібербезпека є доволі нова сфера інформаційної безпеки, яка спрямована на віртуальне середовище, де наразі знаходится суспільство. Термін бере до уваги не тільки захист самої інформації, але й всієї системи в ІТ-полі в цілому. Вона не обмежується тільки захистом інформації, а включає в себе захист від вірусів, хакерських атак, підробки даних тощо. Кібербезпека сьогодні відповідає

за три чинники: суспільство, системи та процеси. Кібербезпека безпосередньо є складовою частиною інформаційної безпеки, бо має ефективні засоби та способи можливої відповіді на агресію у кіберсфері, що може застосовуватись як засіб стримування конфліктів та загроз у кіберпросторі. Отже, кібербезпека посідає важливе місце у інформаційному просторі України, оскільки є станом захищеності інформаційного середовища країни, яке гарантує дотримання прав та законних інтересів особистості, суспільства та держави, надійність, конфіденційність, достовірність даних, забезпечення кіберзахисту та критичної безпеки інфраструктури.

3. Першим з основних законодавчих актів є Закон України «Про основні засади забезпечення кібербезпеки України», який носить більш декларативний характер та не передбачає ні вимог, ні інструкцій щодо запобігання атак. Крім, цього закону було досліджено правову основу кібербезпеки України, через інші нормативно-правові акти, які діють на сьогоднішній день. Цими актами є Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаціно-телекомунікаціних системах» та інші. Другим з основних законодавчих актів є Стратегія кібербезпеки України, що передбачає розроблення та застосування чітко нового законодавства в кіберсфері. Крім, законодавчих актів у сфері кібербезпеки є і нормативно-правові акти, тобто стандарти. На сьогоднішній день в Україні є такі нормативні документи, як НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» та стандарт ICO/IEC 27032. Отже, правове регулювання кібербезпеки в Україні здійснюється відповідними законами та актами, які забезпечують законність, доступність, захищеність кіберсфери.

4. Кіберзлочинність – це протиправне діяння, яке пов'язано з комп'ютерними системами та мережами, де інформація незаконно зберігається, розповсюджуються викрадені бази та банки даних, відбувається несанкціоноване проникнення в роботу комп'ютерних мереж тощо. Існує багато

видів кіберзлочинів, які заважають нормальному функціонуванню систем. Одними з них є правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, зловживання пристроями тощо), правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, правопорушення пов'язанні із змістом інформації (расизм, ксенофобія), правопорушення, пов'язані з порушенням авторських та суміжних прав та інші. Але одним із небезпечних злочинів є кібератака, яка в свою чергу, також поділяється на види. До неї відносяться кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кардшаринг, соціальна інженерія, мальваре, протиправний контент, рефайлінг та інші.

5. На данний момент відкривається шлях до злочинної поведінки і тому можна поділити всю сукупність кіберправопорушників на окремі типи (хакери, кіберзлочинці, шахраї, «білокомірцеві» злочинці та пересічні громадяни). Найбільш поширеним видом кіберзлочинців є хакери – люди, які розуміють самі основи роботи комп'ютерних систем. Існує багато різномінтних видів хакерів: хакер мережевий, кракер, фрікер, кардер, білий капелюх, чорна шапочка, сірий капелюх, хактивіс та найбільш небезпечними є кібертерористи. Кібертероризм спрямований на проникнення цифрової та інформаційно-телекомунікаційної системи, перехоплення управління та інших деструктивних дій. Таким чином, здійснючи відповідні дії кіберзлочинці завдають значної шкоди на локальному, державному та міжнародному рівнях.

6. Заходи протидії є використання засобів фізичного захисту, розробка програмних засобів захисту, шифрування даних, захист інформації від несанкціонованого доступу тощо. На жаль, в Україні боротьба з цими злочинами перебуває на початковому етапі формування, але певну законодавчу базу все створенно, і тому потрібно її дотримуватися та розвивати. Але також не варто забувати про власну кібербезпеку, і тому потрібно дотримуватися певних правил: не завантажувати та не відкривати підозрілі комп'ютерні файли, не

повідомляти стороннім особам свої персональні дані, користуватися антивірусом, створювати складні паролі, не переходити на підозрілі посилання, тримати свої гаджети в полі зору тощо. Виконуючи ці правила безпеки, людина дозволить лише мінімізувати можливість несанкціонованого проникнення.

7. Одним із головних нормативно-правових актів у сфері кібербезпеки є Стратегія розвитку кібербезпеки України, яка була прийнята в 2016 році та стала першою спробою у стратегуванні державної сфери щодо кібербезпеки. Ця стратегія була дійсна до 2020 року, але в 2021 році набрав чинності Указ Президента України «Про рішення Ради національної безпеки і оборони україни «Про стратегію кібербезпеки України»», відповідно до неї держава створюватиме максимально відкритий, вільний та безпечний кіберпростір в інтересах забезпечення прав і свобод людини. Зміст нової Стратегії кібербезпеки України складається з 9 розділів, в яких визначаються шляхи посилення спроможностей національної системи кібербезпеки, показується слабкі і сильні сторони Стратегії 2016 року, формується основні виклики та загрози в сфері кібербезпеки, визначається пріорітерні напрямки забезпечення кібербезпеки, показуються основні стратегічні цілі, які спрямовані на досягнення відповідних стратегічних завдань, визначаються зовнішньополітичні напрямки у сфері кібербезпеки, формується основні критерії результативності виконання Стратегії, показується ефективність здійснення та реалізації Стратегії. Стратегія ставить на меті вирішення нагальних проблем у сфері кібербезпеки, створення умов безпекового функціонування кіберпростору. Ключовими засадами Стратегії є стримування, кіберстійкість та взаємодія, які супроводжуються на досягення стратегічних цілей: дієва кібероборона, ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму, ефективна протидія кіберзлочинності, національна кіберготовність та надійний кіберзахист, безпечні цифрові послуги, зміцнення системи координації, прагматичне міжнародне співробітництво та інші. Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання

стратегічних завдань: запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки, забезпечення максимального охоплення об'єктів критичної інфраструктури негласною перевіркою стану їх готовності до можливих кібератак та кіберінцидентів з метою превентивного усунення передумов до реалізації кіберзагроз, впровадження цифрових послуг для населення та розвиток національної інформаційної інфраструктури тощо. Отже, виконання стратегічних цілей супроводжується виконанням стратегічних функцій (запобігання, захист, мінімізація загроз, реагування, відновлення). Стратегія передбачає створення умов для захисту інформації об'єктів критичної інфраструктури, наукових установ, закладів освіти, організацій, громадських об'єднань і громадян.

8. Основними пріоритетними напрямками Стратегії є : убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства, захист прав, свобод і законних інтересів громадян України у кіберпросторі, європейська і євроатлантична інтеграція у сфері кібербезпеки. Також було визначено головні переваги цієї Стратегії (дотримання європейського підходу до забезпечення кібербезпеки, орієнтація на стандарти ЄС та НАТО в сфері забезпечення кібербезпеки, відмова від пріоритету "захисту національного сегменту Інтернету" тощо). Таким чином, протягом реалізації Стратегії Україна зробить кібербезпеку одним з основних питань своєї діяльності, оскільки відбувається багато кіберправопорушень, які заважають функціонуванню життєдіяльності громадян та створюють перешкоди до розвитку кіберсфери в країні.

Таким чином, завдання вирішенні в повному обсязі, мета досягнута – було здійсненно комплексний аналіз аналіз стратегічного напрямку розвитку кібербезпеки в інформаційному просторі України, висвітлення основних аспектів розуміння проблем системи кіберзахисту та визначення напрямків їх подолання.

У нашому дослідженні ми з'ясували, що кібербезпека є невід'ємною

складовою інформаційного простору. Але комплексна захищеність сталого функціонування інформаційної сфери в інтересах людини, суспільства і держави потребує удосконалення теоретичних, правових і організаційних основ надійного захисту національного кіберпростору. Кібербезпека набуває дедалі більшої ваги та стає одним із найважливіших елементів національної та інформаційної безпеки. Аналіз інформаційного законодавства України, дає підстави стверджувати, що на данний час існує потреба у розробленні якісно нових підходів щодо розуміння правових засад подальшого удосконалення теоретико-правового механізму. Сьогодні триває процес розбудови національної системи кібербезпеки і кіберзахисту, формування її організаційно-технічної моделі, здатної забезпечити оперативне й адекватне реагування на потенційні та реальні кіберзагрози. Тому для кібербезпеки наша країна має вживати таких заходів, як : гарантування своєчасного виявлення зовнішніх загроз, захищеність персональних даних громадян, підвищення рівня міжнародного співробітництва у сфері кібербезпеки, покращити стратегії розвитку кібербезпеки, яка дозволить гарантувати надійність, конфіденційність інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Canada’s Cyber Security Strategy: For a stronger and more prosperous Canada[Електронний ресурс]//Her Majesty the Queen in Right of Canada, 2010. 14 с. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf. (дата звернення: 22.10.2021).

2. Cyber Security Strategy for Germany[Електронний ресурс]//Berlin : Federal Ministry of the Interior. 2011. 15 с. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile. (дата звернення: 22.10.2021).

3. Cyber security strategy[Електронний ресурс]//Commonwealth of Australia: Australian Government, 2009. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf. (дата звернення: 22.10.2021).

4. Information systems defence and security: France’s strategy[Електронний ресурс]//French Network and Information Security Agency. 2011. С. 23. URL: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. (дата звернення: 22.10.2021).

5. National Cyber Security Strategy and 2013-2014 Action Plan[Електронний ресурс]//Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. С. 47. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TUR_CyberSecurity.pdf. (дата звернення: 22.10.2021).

6. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні [Електронний ресурс].URL:https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf (дата звернення: 22.10.2021).

7. Андрусенко С. В. Боротьба з кіберзлочинністю – проблема транснаціонального масштабу[Електронний ресурс]. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/988/1/%D0%90%D0%BD%D0%B4%D1%80%D1%83%D1%81%D0%B5%D0%BD%D0%BA%D0%BE%204-2015.pdf.(дата звернення: 22.10.2021).

8. Бакалінська О. Правове забезпечення кібербезпеки в Україні [Електронний ресурс].//Адміністративне право і процес. К.,2019. №9.С. 100-108.URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf (дата звернення: 22.10.2021)

9. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» [Електронний ресурс] //Правова інформатика. 2014. №2. URL: http://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya-%E2%80%9Ckiberbezpeka%E2%80%9D. (дата звернення: 22.10.2021).

10. Безуглий Д. Інформаційна безпека України: огляд останніх тенденцій[Електронний ресурс] // Фізико-математична освіта.2018.№ 2(16). С. 13–17. URL: https://cyberleninka.ru/article/n/informatsiyna-bezpeka-ukrayini-oglyad-ostannih-tendentsiy1/viewer (дата звернення: 22.10.2021).

11. Бурячко В. Л. Інформаційна та кібербезпека: соціотехнічний аспект[Електронний ресурс]//Державний університет телекомунікацій. 2015.288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf. (дата звернення: 22.10.2021).

12. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Електронний ресурс]// Державний університет телекомунікацій. К. : ТОВ «СІК ГРУП Україна», 2015. 449 с. URL:http://www.dut.edu.ua/uploads/p_303_32151446.pdf. (дата звернення: 22.10.2021).

13. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.

14. Валюшко О.І. Кібербезпека України: наукові та практичні виміри сучасності [Електронний ресурс]//Дипломатична академія України при МЗС України. К.,2016. URL: http://visnyk-psp.kpi.ua/article/view/140496/137578. (дата звернення: 22.10.2021).

15. Види хакерів [Електронний ресурс]. URL: https://sites.google.com/site/hakerovnet34/home/vidy-hakerov. (дата звернення: 22.10.2021).

16. Волох О.К. Питання кібернетичної безпеки в умовах формування інформаційного суспільства [Електронний ресурс]. URL: http://lsej.org.ua/4_2016/29.pdf. (дата звернення: 22.10.2021).

17. Галинська К. Ю. Стратегія кібербезпеки як основа інформаційного правопорядку в Україні [Електронний ресурс] // Національний юридичний університет ім. Я.Мудрого. К., 2013. URL: https://revolution.allbest.ru/law/00853955_0.html. (дата звернення: 22.10.2021).

18. Горовий С.С. Актуальні питання правового забезпечення кібербезпеки України [Електронний ресурс] // Юридичний науковий електронний журнал.К.,2021.№ 6.С. 120-122. URL: http://www.lsej.org.ua/6_2021/34.pdf. (дата звернення: 22.10.2021).

19. Грібоєдов С. М. Удосконалення державного планування у сфері забезпечення кібербезпеки в умовах гібридних загроз [Електронний ресурс]// Інформація і право. К.,2021. №1. С. 114-122. URL: http://ippi.org.ua/sites/default/files/15_17.pdf. (дата звернення: 22.10.2021).

20. Демедюк С.В. Окремі питання адміністративно-правововго та організаційного забезпечення кібербезпеки [Електронний ресурс] // Південно-український правничий часопис. К., 2015. № 2. С. 144-147. URL: http://www.sulj.oduvs.od.ua/archive/2015/2/44.pdf. (дата звернення: 22.10.2021).

21. Демидов З. Основні види кібератак на wed-сайти [Електронний ресурс]. URL: http://ippi.org.ua/sites/default/files/5_11.pdf. (дата звернення: 22.10.2021).

22. Дзяна Г. Реалізація національної політики у сфері кібербезпеки [Електронний ресурс]. URL:http://www.lvivacademy.com/vidavnitstvo_1/edu_48/fail/14.pdf. (дата звернення: 22.10.2021).

23. Діодріца І. Поняття та зміст національної системи кібербезпеки [Електронний ресурс]//Національний юридичний журнал: Теорія і практика.К.,2016. URL: http://www.jurnaluljuridic.in.ua/archive/2016/6/part_1/9.pdf. (дата звернення: 22.10.2021).

24. Діордіца І. В. Поняття і зміст кібертероризму [Електронний ресурс]. URL:http://www.pjv.nuoua.od.ua/v3_2016/15.pdf. (дата звернення: 22.10.2021).

25. Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави [Електронний ресурс]// Інформація і право. К., 2017. №1. С. 104-111. URL: http://ippi.org.ua/sites/default/files/13_3.pdf. (дата звернення: 22.10.2021).

26. Дубов Д. В. Формуючи нову стратегію кібербезпеки України: Чи можемо уникнути помилок першої спроби стратегування? [Електронний ресурс]//Національний інститут стратегічних досліджень.К.,2021.С.1-6. URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf. (дата звернення: 22.10.2021).

27. Закон України «Про основні засади забезпечення кібербезпеки України»: (офіц. текст: за станом на 05.10.2017)[Електронний ресурс]// Верховна Рада України.Київ, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 22.10.2021).

28. Запорожець О.Ю. Політика європейського союзу в сфері інформаційної безпеки» [Електронний ресурс]. URL: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/1195/1139. (дата звернення: 22.10.2021).

29. Захист інформації в системах електронного урядування[Електронний ресурс]. URL: https://onat.edu.ua/wp-content/uploads/2018/05/Part_013_Feb_2018.pdf. (дата звернення: 22.10.2021).

30. Інформаційна безпека [Електронний ресурс]. URL: https://studopedia.su/16_59389_Informatsiyna-bezpeka.html. (дата звернення: 22.10.2021).

31. Інформаційна безпека і кібербезпека - в чому різниця? [Електронний ресурс]. URL:https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/. (дата звернення: 22.10.2021).

32. Кіберзлочинність в Україні [Електронний ресурс]. URL: https://equity.law/press-center/publications/1169.html.(дата звернення: 22.10.2021).

33. Кіберзлочинність в усіх її проявах [Електронний ресурс]. URL: https://gurt.org.ua/articles/34602/.(дата звернення: 22.10.2021).

34. Кіберполіція [Електронний ресурс].URL: https://wiki.legalaid.gov.ua/index.php/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%8F._%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8(дата звернення: 22.10.2021).

35. Комп'ютерна безпека [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0#:~:text=%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D1%94%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%BE%D1%8E%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8,%D0%BA%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%B0%D1%85%20%D1%82

%D0%B0%20%D1%96%D0%BD%D1%88%D0%B8%D1%85%20%D0%BF%D1%80%D0%B8%D1%81%D1%82%D1%80%D0%BE%D1%8F%D1%85. (дата звернення: 22.10.2021).

36. Кондратюк М.В. Кібербезпека України в системі національної безпеки [Електронний ресурс]// Право і суспільство. К., 2019.№ 6 (частина 2). С. 42-48. URL: http://pravoisuspilstvo.org.ua/archive/2019/6_2019/part_2/9.pdf. (дата звернення: 22.10.2021).

37. Кундеус В. Поняття та види кіберзлочинів [Електронний ресурс]. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/7723/Poniattia_Kundeus_2020.pdf?sequence=1&isAllowed=y. (дата звернення: 22.10.2021).

38. Куцаєв В.В. Розширення термінології сучасного кіберпростору [Електронний ресурс]. URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc. (дата звернення: 22.10.2021).

39. Ліпкан В. [Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України Електронний ресурс]// Підприємство, господарство і право.К.,2017.№5.С. 174-180. URL: http://www.pgp-journal.kiev.ua/archive/2017/5/40.pdf.(дата звернення: 22.10.2021).

40. Микитенко Д. О. Захист інформації та кібербезпека як складова частина національної безпеки України [Електронний ресурс] // Юридичний науковий журнал;Національний юридичний університет ім. Я. Мудрого. Київ,2020.№8. с. 381-385. URL: http://www.lsej.org.ua/8_2020/96.pdf. (дата звернення: 22.10.2021).

41. Національна стратегія кібербезпеки (NCSS).Від розуміння до можливостей[Електронний ресурс]//Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. URL: https://english.nctv.nl/topics/national-cyber-security-agenda/documents/publications/2018/06/07/national-cyber-security-agenda. (дата звернення: 22.10.2021).

42. Нікулеско Д. Кібербезпека: вразливі моменти[Електронний ресурс]. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html. (дата звернення: 22.10.2021).

43. Нова Стратегія кібербезпеки України [Електронний ресурс].URL: https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/(дата звернення: 22.10.2021).

44. Петров В. Підходи до концептуальних засад проєкту Стратегії кібербезпеки України на 2021–2025 роки[Електронний ресурс] // Незалежний аналітичний центр геополітичних досліджень. К., 2021. URL: https://bintel.org.ua/analytics/voenni-voprosy/armii-voorugenie/konceptualni-zasadu-proyektu-strategii-kiberbezpeki-ukraini-na-2021-2025-roki/.(дата звернення: 22.10.2021).

45. Піратство в Інтернеті [Електронний ресурс]. URL: https://apo.kiev.ua/internet.phtml. (дата звернення: 22.10.2021).

46. Правові аспекти кібербезпеки бізнесу [Електронний ресурс]. URL: https://cpk.ua/uk/publikatsiyi/statti-publikatsiyi/full/pravovi-aspekti-kiberbezpeki-biznesu/.(дата звернення: 22.10.2021).

47. Проект «Стратегія кібербезпеки України (2021-2025 роки)» [Електронний ресурс]// Рада національної безпеки і оборони України. К., 2021. 27 с. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf. (дата звернення: 22.10.2021).

48. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні [Електронний ресурс].URL: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka.pdf(дата звернення: 22.10.2021).

49. Пфо О. Основні поняття та класифікація кіберзлочинів [Електронний ресурс]. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5119/1/AUConferenceCyberSecurity_November2016_p33.pdf. (дата звернення: 22.10.2021).

50. Рекомендація Ради національної безпеки і оборони України щодо заходів кібербезпеки[Електронний ресурс]. URL:

https://if.dsns.gov.ua/files/2020/slugbova%20lekzii/2020/prof/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%8F%20%D0%A0%D0%B0%D0%B4%D0%B8%20%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D1%96%20%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8%20%D1%89%D0%BE%D0%B4%D0%BE%20%D0%B7%D0%B0%D1%85%D0%BE%D0%B4%D1%96%D0%B2%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8.pdf . (дата звернення: 22.10.2021).

51. РНБО схвалили проєкт Стратегії кібербезпеки України на 2021–2025 роки[Електронний ресурс].URL: https://armyinform.com.ua/2021/03/04/u-rnbo-shvalyly-proyekt-strategiyi-kiberbezpeky-ukrayiny-na-2021-2025-roky/(дата звернення: 22.10.2021).

52. Стратегія кібербезпеки України [Електронний ресурс]. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_prezentaciya.pdf . (дата звернення: 22.10.2021).

53. Стратегія кібербезпеки України: цілі та пріорітери [Електронний ресурс]. URL: https://armyinform.com.ua/2021/08/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.(дата звернення: 22.10.2021).

54. Сучасний стан забезпечення кібербезпеки в Україні [Електронний ресурс]. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/290/1/%D0%A1%D0%A3%D0%A7%D0%90%D0%A1%D0%9D%D0%98%D0%99%20%D0%A1%D0%A2%D0%90%D0%9D%20%D0%97%D0%90%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%A7%D0%95%D0%9D%D0%9D%D0%AF%20%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%9

8%20%D0%92%20%D0%A3%D0%9A%D0%A0%D0%90%D0%87%D0%9D%D0%86.pdf. (дата звернення: 22.10.2021).

55. Типи комп'ютерних хакерів[Електронний ресурс]. URL: https://glennbouchard.com/uk/361-tipe-tipe-hacker-komputer.html. (дата звернення: 22.10.2021).

56. Трофименко О. Кібербезпека України: аналіз сучасного стану [Електронний ресурс] //Захист інформації, том 21. №3.2019.С. 150-158. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y. (дата звернення: 22.10.2021).

57. Форос Г. В. правові основи захисту інформації в кіберпросторі [Електронний ресурс]. URL: http://pd.onu.edu.ua/article/view/132891. (дата звернення: 22.10.2021).

58. Хакери [Електронний ресурс]. URL: https://znaimo.com.ua/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80.- Назва з титул. екрана. (дата звернення: 22.10.2021).

59. Цюцюра С.В. Дослідження сфери кібербезпеки в Україні [Електронний ресурс]// Київ. нац. торг.-екон. ун-т. Rbїd?2020/ С/ 46-48/ URL:https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf. (дата звернення: 22.10.2021).

60. Чаплик М. Український вимір кіберзлочинності [Електронний ресурс]. URL:http://habitus.od.ua/journals/2020/11-2020/16.pdf. (дата звернення: 22.10.2021).

61. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління[Електронний ресурс] //Державне управління у сфері національної безпеки . URL: http://mino.esrae.ru/pdf/2015/Ref/1484.pdf. (дата звернення: 22.10.2021).

62. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення[Електронний ресурс]. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2012_2_36.pdf . (дата звернення: 22.10.2021).

63. Що таке фішинг і як від нього захиститись? [Електронний ресурс]. URL: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html. (дата звернення: 22.10.2021).

64. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни [Електронний ресурс]. URL:http://lib.nadpsu.edu.ua/eldocs/BooksShow8/Nvnudpsu_2014_2_10.pdf. (дата звернення: 22.10.2021).