МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА
РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Ніна РЖЕВСЬКА
«15» 06 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
ЗА СПЕЦІАЛЬНІСТЮ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО - ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ДЕРЖАВНА ПОЛІТИКА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ»

Виконавець: здобувач вищої освіти 4 курсу, 409 групи, Лавник Аліна Михайлівна

Керівник: к. політ.н., доцент кафедри міжнародних відносин, інформації та регіональних студій Мороз Андрій Сергійович

Нормоконтролер: _____ Олексій МЕНДРІН
(підпис)

КИЇВ 2023

ЗМІСТ

ВСТУП

Актуальність теми. Поряд із злочинами проти людства, національної безпеки та миру є злочин кіберзлочинність. В умовах стрімкого розвитку технологічного процесу, розвитку комп'ютерних технологій, впровадження інтернету в звичний ритм життя людини спостерігається як полегшення комунікацій, так і створюються проблеми захисту персональних даних. Банківська сфера, соціальні мережі, смартфони та додатки до них – це все простір для кіберзлочинців. До того ж, кіберзлочинці є не тільки комп'ютерними геніями, а й звичайними споживачами інтернет-технологій. Шахраї постійно реалізують нові схеми злочинності, при цьому використовуючи безпосередній контакт по телефону та заходячи на персональні сторінки потенційних жертв. Найпопулярнішими видами злочинів є «розведення» на гроші. Представляючись робітниками банків, шахраї збирають особисті дані для викрадення грошей. Для цього банки постійно працюють над захистом рахунків своїх клієнтів, створюючи розгалужену систему захисту баз даних. Кібератакам піддаються й державні органи, що несе безпеку національній безпеці країни. Приватний сектор, бізнес, також є об'єктом атак потенційних кібершахраїв. Кіберзлочинність – це масштабне явище, тому важливим для кожної країни є сумісна співпраця та обмін досвідом в кібербезпеці. В умовах сьогоднішньої військової агресії з боку росії, для України вкрай важливим є захист свого кіберпростору та інформпростору.

Аналіз останніх досліджень і публікацій. Окремі аспекти боротьби та протидії кіберзлочинності розглядаються в роботах спеціалістів в даній сфері. Зокрема, цій проблематиці присвячено роботи вітчизняних науковців В.В.Маркова,М.О.Будакова,В.М.Бутузова, В.В.Коваленко, Я.Ю.Кондратьєва, Ю.Є.Максименко, А.І.Марущаком та іноземними фахівцями А.Робертом, К.Осакве, Т.Блентаном, Д.Банісаром та ін. Уперше питання кіберзлочину підняв американський вчений Донн Б. Паркер (США). Він ще у другій

половині двадцятого сторіччя досліджував поняття кіберзлочину. Донн Б. Паркер є розробником права щодо комп'ютерних злочинів.Після цього дане керівництво досі використовується як енциклопедія поза межами Сполучених штатів Америки. Поряд із Донн. Б. Паркером досліджували питання кіберзлочину ще й інші науковці США Аугуст Беквейс та Джей Блуумбекер . Звичайно, європейські вчені також досліджували явище кіберзлочину. Так, Штайн Шольберг, який працював в Інтерполі та був прокурором Норвегії, розробляв концепцію кіберзлочину. Німецький професор Університету в Фрайбурзі Урліх Зібер працював в міжнародних організаціях таких як ООН, ОБСЄ та працював над втіленням захисту у кіберпросторі. Нідерландський науковець Х.В.К. Касперсен є одним з основоположників конвенції х боротьби з кіберзлочинністю.

Метою роботи є розгляд державної політики в протидії кіберзлочинності в умовах інформаційної війни рф проти України.

Відповідно до мети були поставлені і вирішені наступні **завдання:**

- провести теоретичний та методологічний аналіз терміну «кіберзлочинність»;
- виявити способи і види кіберзлочинів;
- проаналізувати інструменти протидії кіберзлочинності в умовах інформаційної війни;
- розглянути сутність, мету державної політики та принципи за якими діє держава при створенні умов запобігання кіберзлочинності та які завдання покладені на державу у вирішенні цього питання;
- скласти організаційно-технічну модель забезпечення кібернетичної безпеки України;
- оцінити та визначити роль кібернетичних атак в інформаційній війни рф проти України;

- визначити проблеми та перспективи вдосконалення дій з боку держави задля забезпечення безпеки в кіберпросторі в України;
- виокремити роль міжнародного середовища у протидії кіберзлочинності в України;
- розглянути виклики глобальній кібернетичній безпеці як наслідок інформаційної війни рф проти України та шляхи їх подолання.

Об'єктом дослідження є дослідження виявлення і протидії кіберзлочинів з боку держави, на основі оцінки та ролі кібернетичних атак та з урахуванням досвіду боротьби із даним видом злочину в міжнародному середовищі.

Предметом дослідження є визначення, проявів, визнання кіберзлочинності, визначення процесів кіберзлочину, державна політика протидії кіберзлочинності в умовах інформаційної війни рф проти України.

Практичне значення отриманих результатів впливає на виявлення пробілів в законодавстві з державного регулювання трактовки кіберзлочинів, розробка механізмів щодо навчання спеціалістів з кіберзлочинності саме в діючих умовах російської агресії та зупинення російських атак на комп'ютерну мережу в Україні, враховуючи досвід міжнародних організацій.

Методи дослідження ґрунтуються на опрацьованих положеннях методології визначення кіберзлочинів. У процесі роботи використовувалися методи аналізу – при аналізі сутності кіберзлочинності в умовах військової агресії з боку рф. Метод аналізу передбачає збір, обробка та здійснення висновків на основі даних дослідження.

Інформаційною базою роботи була статистична, галузева інформація в області кіберпростору, наукові роботи, публікації в пресі, результати самостійних висновків на основі теоретичного та практичного матеріалу. Апробація результатів роботи полягає в тому, що результати дослідження представлено на науково– практичній конференції XXI Міжнародна науково–практична конференція «ПОЛІТ. Сучасні проблеми науки» у галузі міжнародних відносин (м. Київ, НАУ, 10 березня 2022 року).

Структура роботи. Випускна кваліфікаційна робота складається зі вступу, 3 розділів, висновків, списку використаних джерел, додатків. Робота викладена на 55 сторінках, містить 2 таблиці, 7 рисунків, додатки. Список використаних джерел налічує 41 позицію.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ПРОТИДІЇ КІБЕРНЕТИЧНІЙ ЗЛОЧИННОСТІ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Кіберзлочинність як предмет дослідження: теоретичний та методологічний аналіз

Під терміном «кіберзлочинність» слід розуміти вид злочину, здійснений за допомогою комп'ютерної техніки, смартфону та інших спеціальних технічних засобів, що призводить до шахрайства в мережі, використанні неліцензійних програм та інших видів злочину.

Як наголошує кандидат юридичних наук В. В. Марков, кіберзлочин є однією з найбільших проблем сучасності, з якою вимушено зіткнулося людство не зважаючи в якій країні відбувся злочин. Таке становище речей постійно буде загострюватись, оскільки технологічний процес не стоїть на місці. [14]

Розвиток технологічного прогресу відбувається набагато швидше від розвитку нормативно-правової бази щодо злочинів в кіберпросторі, тому реакція на такі злочини може бути неоднозначною.

Як стверджує В.М. Бутузов, поняття кіберзлочинність вживається поряд із терміном «комп`ютерна злочинність». Ці два поняття тотожні, але кіберзлочинність значно ширша, оскільки охоплює не лише комп'ютерний простір а й телекомунікаційні мережі і взагалі увесь інформаційний простір.

В своїх думках про сутність кіберзлочинності мають схожість тлумачення іноземних вчених А. Роберта та К. Осакве – кіберзлочинність – це протиправні дії, які здійснюються особами, з метою умисного злочину, з використанням комп'ютерних технологій, задля викрадення матеріальних чи інтелектуальних цінностей [14]. Під шахрайські дії кіберзлочинів можуть підпадати як держава так і звичайні люди або бізнес.

Якщо звернутись до оксфордського словника, то ми побачимо що приставка «cyber» є частиною складного слова. Значення цього слова належить IT-технологіям, Інтернету, віртуальної реальності тощо. А «cybercrime», за версією Кембриджського університету це вже злочинність в комп`ютерній мережі та за допомогою засобів пов’язаних з комп’ютерами. У той же час термін «computer crime» в основному стосується злочинів, які скоєні щодо комп’ютерів або комп’ютерних даних. Міжнародне право закріпило терміни «кіберзлочинність» і «комп`ютерна злочинність». Прийнята Конвенція про кіберзлочинність Радою Європи в листопаді 2011 року в своїй преамбулі вживає поняття «cybercrime», а не «computer crime» [13]. Необхідно відмітити, що офіційного визначення кіберзлочину у міжнародній спільноті поки що немає.

Разом з тим, аналіз внутрішнього законодавства України, що регулює суспільні інформаційні відносини, свідчить, що Україна вживає всіх необхідних заходів, спрямованих на запобігання та протидію комп'ютерній злочинності. Прикладами таких заходів є Указ Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 31 липня 2000 року та стаття 16 чинного Кримінального кодексу України "Про електронно-обчислювальні машини (комп'ютери), системи та правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів),систем та комп'ютерних мереж". Однак, лише цим не можна повністю подолати кіберзлочинність у нашій країні.

Авторське формулювання терміну «кіберзлочинність» можна визначити таким чином.

Отже, під «кіберзлочинністю» пропонується розуміти:

– незаконні, умисні вчинки, предметом здійснення злочину яких є інфотехнології, а об’єктом будь-які цінності жертви кіберзлочину;

– незаконне втручання в роботу кібернетичних систем, основним об'єктом управління яких є комп'ютер (наприклад, спотворення інформації про

стан об'єктів у каналах зворотного зв'язку, спотворення сигналів управління та каналів зв'язку, використання шкідливого програмного забезпечення; використання існуючих кібернетичних (комп'ютерних) систем у злочинних цілях (наприклад, комп'ютерних або телекомунікаційних мереж при шахрайстві, вимаганні тощо) [10,с.85]; це визначення може бути використано як приклад при прийнятті відповідних нормативно-правових актів;

– правопорушення, вчинені за допомогою або з використанням комп'ютерних систем, або правопорушення, пов'язані з комп'ютерними системами, тобто сукупністю одного або декількох пристроїв, що виконують автоматичну обробку даних за певною програмою[11].

– протиправні дії в ІТ-просторі 4,с.89], тобто з використанням текстової, графічної або іншої інформації (даних), яка існує в електронній формі, зберігається на відповідному носії і може бути створена, змінена або використана за допомогою комп'ютера;

– суспільно небезпечне кримінальне правопорушення, визначене Кримінальним кодексом, яке полягає в незаконному використанні інформаційно-комунікаційних технологій [1];

– сукупність злочинів, що вчиняються в комп'ютерних мережах та віртуальному чи інфопросторі [11, С.267];

– злочини у просторі комп'ютерних і телекомунікаційних мереж [1, С. 190].

Конвенція про кіберзлочинність від 1 липня 2006 року також не містить визначення поняття «кіберзлочинність». Водночас, у її преамбулі зазначено, що Конвенція необхідна для запобігання діям, спрямованим проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також неправомірному використанню таких систем, мережі даних, і для встановлення кримінальної відповідальності за такі дії. У ньому зазначено, що необхідно запобігати неправомірному використанню систем, мережі даних.

Як передбачено в Конвенції, криміналізувати такі діяння та надати достатні повноваження для ефективної боротьби з такими злочинами шляхом сприяння їх виявленню, розслідуванню та переслідуванню на національному та міжнародному рівнях, а також вжити заходів для швидкого та надійного міжнародного співробітництва [4].

Таким чином, у цьому контексті кіберзлочинність включає незаконний доступ, незаконне перехоплення, втручання в дані або системи, неправомірне використання обладнання, шахрайство, злочини, пов'язані з дитячою порнографією, порушення авторського права та суміжних прав, злочини проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також неправомірне використання цих систем, мережі даних, що визначаються як діяння, за які передбачена кримінальна відповідальність [9].

Підсумовуючи вищесказане, по - перше, комп'ютери, тобто комп'ютерні мережі та комп'ютерні системи, є засобами, за допомогою яких вчиняються кіберзлочини. З точки зору кримінального права вони характеризуються прямим умислом, що значною мірою виключає можливість необережності. Крім того, об'єктом злочину є звичайна фізична особа. Цей вид злочинів спрямований на порушення роботи інформаційних і комп'ютерних систем, порушення авторських і суміжних прав, незаконну діяльність з використанням засобів доступу до банківських рахунків, таких як документи на переказ грошей і платіжні картки, а також обладнання для їх виготовлення.

Наслідки кіберзлочинності зачіпають інтереси не лише окремих жертв, але й компаній, організацій, урядів і суспільства в цілому. Кіберзлочинність часто компрометує життєво важливу інформацію та об'єкти критичної інфраструктури, які в багатьох країнах не контролюються державним сектором, і такі злочини можуть мати дестабілізуючий вплив на всі сектори суспільства. Тому слід стверджувати, що кіберзлочинність є загрозою національній безпеці в кіберпросторі.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав; шахрайство; засоби доступу до банківських рахунків, у тому числі документів на переказ та платіжних карток; незаконне використання обладнання для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів); ввезення, виготовлення, збут і розповсюдження порнографічних предметів; використання та використання відомостей, що становлять комерційну та банківську таємницю у тому числі незаконне збирання такої інформації з метою[6].

Проаналізувавши теоретичні та практичні дослідження у сфері визначення поняття кіберзлочинності, можна зробити висновок, що серед сучасних українських науковців не існує єдиного підходу до визначення поняття кіберзлочинності. Більше того, підходи досить суттєво відрізняються, що може призвести до непорозумінь і, в свою чергу, до неправильної ідентифікації злочинних діянь, що є проблематичним не тільки з теоретичної, але й з практичної точки зору.

1.2. Способи і види кібернетичних злочинів, як один із видів загроз інформаційній безпеці

Кіберзлочини можна класифікувати відповідно до їхньої мети, виконавця та способу вчинення.

Наразі найпоширеніша класифікація кіберзлочинів базується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація наразі слугує "еталоном", оскільки існуючі міжнародні, регіональні документи та наукові практики використовують цю класифікацію.

1) Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

- Несанкціонований доступ – умисний несанкціонований доступ до всієї або частини комп'ютерної системи, з метою отримання комп'ютерних даних або з будь-якою іншою неналежною метою;
- Втручання в дані – навмисне пошкодження, знищення, спотворення, зміна або приховування комп'ютерних даних без належних на те прав;
- Системне втручання – навмисне і суттєве втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, спотворення, зміни або приховування комп'ютерних даних без належних на те прав;
- Незаконне використання пристрою, тобто його виготовлення, продаж, придбання з метою використання, розповсюдження або надання в користування іншим способом;

2) Правопорушення, пов'язані з комп'ютером

3) Правопорушення, пов'язані з контентом

4) Правопорушення, пов'язані з порушенням авторського права та суміжних прав[2];

5) Акти расизму та ксенофобії, вчинені через комп'ютерні мережі [5].

Основними видами кіберзлочинів є розповсюдження шкідливих програм, злам паролів, крадіжка номерів кредитних карток та іншої банківської інформації, а також поширення незаконної інформації через Інтернет [12].

Групи кіберзлочинів поділяються за метою правопорушення на: злочини, що порушують конфіденційність, цілісність і доступність комп'ютерних даних та комп'ютерних мереж; економічні комп'ютерні злочини; комп'ютерні злочини проти недоторканності прав особи та приватного простору; комп'ютерні злочини проти суспільних та державних інтересів проти комп'ютерних злочинів. Однак варто зазначити, що багато кіберзлочинів впливають на декілька об'єктів одночасно. Ще однією категорією правопорушень, яка окремо не згадується в Конвенції Ради Європи (і яка набула значного поширення після прийняття Конвенції), є крадіжка особистих даних, тобто викрадення, передача або використання персональних даних у злочинних цілях [15].

Сьогодні прийнято класифікувати кіберзлочини наступним чином:

1) Наступальні – кібертероризм, погрози фізичного насильства (наприклад, надіслані електронною поштою), кіберпереслідування, кіберсталкінг (незаконні сексуальні домагання або переслідування інших осіб через Інтернет), дитяча порнографія (створення порнографічних матеріалів із зображень дітей); розповсюдження цих матеріалів, отримання доступу до них);

2) Неагресивні – кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство, спам та віруси [27].

Водночас, беручи до уваги мотиви правопорушників, кіберзлочини можна класифікувати наступним чином:

- Кібершахрайство, спрямоване на отримання коштів;
- Кібершахрайство, спрямоване на отримання інформації (для особистого використання або продажу); та втручання в інформаційні системи для отримання доступу до автоматизованих

систем управління (з метою отримання винагороди або нанесення шкоди конкуренту);

- Кіберзлочини, які стосуються інформаційної безпеки держави;
- Кіберзлочини, що направлені на знищення даних;
- Кіберзлочини, що направлені на порушення роботи інформаційних систем у приватному секторі;
- Кіберзлочини, що трактуються як несанкціонований доступ на приватні сторінки користувачів соціальних мереж, тощо;
- Інші злочини.

Крім того, деякі з найпоширеніших кіберзлочинів включають скімінг карток, фішинг, вішинг, онлайн– шахрайство, хакерство, спільне використання карток, соціальну інженерію, переслідування, незаконний контент і рефайлінг [6].

Наступні прояви кіберзлочинності є дуже поширеними сьогодні.

Ці злочини відбуваються в кіберпросторі або комп'ютерних мережах. Кіберпростір – це комп'ютерно-модульований кіберпростір, що містить персональну інформацію або події і процеси, виражені в математичній, символьній або іншій формі. Ця інформація зберігається в пам'яті фізичних або віртуальних пристроїв, призначення яких її зберігання, обробки та передачі в процесі переміщення локальними та глобальними комп'ютерними мережами.

Кіберзлочини вчиняються до комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних, використання комп'ютерних систем або доступу до комп'ютерних мереж кіберпростору. Тому комп'ютери можуть бути як знаряддям вчинення злочину, так і об'єктом злочину [14].

В. Бутузов, науковець, який займається проблематикою кіберзлочинності, у своїй роботі звертає увагу на такі особливості кіберзлочинності:

1) Важливість віднесення деяких злочинів у сфері новітніх інформаційних технологій до комп'ютерних полягає у знарядді вчинення

злочину – комп'ютерній техніці. Об'єктом злочину є суспільні відносини у сфері автоматизованої обробки інформації;

2) Значення віднесення окремих правопорушень у сфері новітніх інформаційних технологій до кіберзлочинів полягає в особливому середовищі, в якому вчиняється правопорушення – кіберпросторі (середовищі комп'ютерних систем та мереж). При цьому предмет злочинної агресії може стосуватися будь-якої сфери людської діяльності, яка проявляється в кіберпросторі. При цьому дослідник посилається на перелік протиправних діянь, передбачених Конвенцією та Додатковими протоколами до неї. За його словами, лише діяння з цього переліку класифікуються як кіберзлочини [6, с. 119].

Відсутність легального визначення призводить до певних дискусій. Наразі правове регулювання кіберзлочинності не встигає за сучасним розвитком інформаційних технологій, що загострює проблему кіберзлочинності та робить її реальною загрозою національній безпеці України. Що стосується фізичних осіб, то кіберзлочинність пов'язана з використанням піратського програмного забезпечення, яке дозволяє зловмисникам отримати доступ до персональних даних. Піратство також створює надзвичайно сприятливі умови для виникнення та розвитку кіберзлочинності.

Питання запобігання кіберзлочинності в Україні є комплексним. Сьогодні законодавство має бути адаптоване до сучасних реалій, а не до рівня розвитку науки чи розуміння правлячою групою пріоритетності тих чи інших національних інтересів. Технологічний розвиток, кібернетизація та подальше впровадження штучного інтелекту в наше життя – це вже не майбутнє, а сьогодення.

1.3. Інструменти протидії кіберзлочинності в умовах інформаційної війни

Оскільки кіберзлочинність є транснаціональною за своєю природою, більшість науковців вказують на максимальний рівень затримки як на характеристику кіберзлочинності. Факторами, що сприяють затримці кіберзлочинності, є

1) Складність і масштабність механізмів кіберзлочинності та широкий спектр наслідків, а також "комп'ютерна неграмотність" багатьох потенційних жертв кіберзлочинності та нехтування питаннями безпеки;

2) Негативна поведінка жертв (свідків) злочинів – потерпілі або особи, які володіють інформацією про злочин, не повідомляють про правопорушення або про вчинення кіберзлочину правоохоронним органам;

3) Існують недоліки в роботі правоохоронних органів щодо реагування на заяви або повідомлення про кіберзлочини.

Існує три різні напрямки заходів боротьби з кіберзлочинністю: загально соціальні заходи, специфічні кримінологічні заходи та індивідуальні заходи.

Заходи протидії на загально соціальному рівні кіберзлочинності включає комплекс перспективних соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на розв'язання нагальних соціальних проблем і протиріч у країні. Саме реалізація загально соціальних профілактичних заходів здатна усунути або мінімізувати дію криміногенних факторів, що детермінують кіберзлочинність та гальмують розвиток особистості злочинців.

Розробка належних заходів протидії злочинності, в тому числі кіберзлочинності, потребує належної регламентації діяльності як правоохоронних органів, так і вищих органів державної влади, що, в свою чергу, відповідає вимогам правової, незалежної та демократичної держави.

Також необхідно усунути фактори, які сприятливо впливають на існування та розвиток злочинності [8].

Професійне запобігання злочинності безпосередньо пов'язане з діяльністю Національної поліції України та спрямоване переважно на певні соціальні групи, які привертають увагу об'єктів профілактичної діяльності.

Основними заходами щодо запобігання кіберзлочинності, які здійснюються ОВС та Національною поліцією (в особі Департаменту кіберполіції), є розробка та затвердження Міністерством внутрішніх справ стратегії боротьби з кіберзлочинністю. Ця стратегія має включати концепцію діяльності із запобігання злочинам, стратегічні з точки зору науки та тактичні заходи запобігання злочинам, а також механізм моніторингу їхньої якості. Збільшити кількість регулярних та нерегулярних перевірок відповідними органами поліції компаній, діяльність яких безпосередньо пов'язана з кіберзлочинністю.

Потенційно небезпечні шахраї повинні бути розпізнані і про поведінку яких свідчить систематичне переписування несуттєвих даних, модифікація або видалення даних, поява неправдивих записів тощо, також має бути визначено як один з аспектів діяльності з протидії кіберзлочинності.

Ще одним заходом запобігання кіберзлочинності є виявлення та запобігання діяльності кібертерористів, тобто тих, хто використовує комп'ютерне обладнання, пристрої та мережі для вчинення терористичних актів.

В умовах інформаційної війни під час діючої військової агресії з боку росії, найбільш вразливі до кібератак є державні установи, великі корпорації, оборонні підприємства та підприємства критичної інфраструктури, а також компанії, які забезпечують все необхідне для населення та оборони у воєнний час.

Не виключається ризик для звичайної людини, яка може і не знати про скоєний злочин в її бік.

Військовий стан передбачає використання інструментів протидій кіберзлочинів:

1. Наявність у штаті держорганів, підприємств висококваліфікованого спеціаліста у сфері ІТ. Професіонали мають здатність вчасно розпізнавати атаки з боку агресора та знешкоджувати їх. ІТ-спеціаліст має роз'яснити правила поведінки у комп'ютерній мережі для інших працівників.

2. Тим, хто перебуває в зоні кіберризику, слід стежити за відповідними повідомленнями на офіційних ресурсах Адміністрації Дер спецзв'язку та CERT-UA. Ці установи публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати ризики.

3. У разі кібератаки інформувати спеціалізовані органи, відповідальні за виявлення та протидію цим злочинам.

4. Як тільки атака виявлена, найважливіше завдання – повідомити про неї офіційні органи кібербезпеки України – CERT-UA та Кіберполіції. Це дозволить не лише притягнути винних до відповідальності, але й забезпечити негайне вжиття заходів щодо блокування шкідливого веб– ресурсу.

5. Особи, які здійснюють кібератаки проти ворожих держав або займаються багхантингом для посилення кібербезпеки України у воєнний час, повинні бути готові довести, що їхня діяльність відповідає інтересам України, щоб уникнути непорозумінь з правоохоронними органами.

Підсумовуюче викладене в першому розділі, можна сказати, що природу кіберзлочинів почали досліджувати американські вчені ще в 70– ті роки минулого сторіччя. Із розвитком комп'ютерних технологій, розвивалися і злочини в мережах. Розповсюдження Інтернету надало можливість шахраям, за допомогою мережі, здійснювати різні види кіберзлочинів. Ототожнюючи всі поняття, які були досліджені вітчизняними та іноземними вченими, можна сказати, термін "кіберзлочинність" означає правопорушення у сфері комп'ютерної інформації та телекомунікацій, незаконну торгівлю бездротовими електронними та спеціальними технічними засобами, несанкціоноване розповсюдження комп'ютерного програмного забезпечення та інші види правопорушень. Існує безліч способів і видів кіберзлочинів. Якщо ототожнити способи – це шахрайські дії через мережу Інтернет, телефонні

мережі з метою отримання прибутку для шахраїв або нанесення шкоди державним органам, підприємствам або фізичним особам з метою їх дискредитації. В умовах війни із рф та інформаційної війни із країною агресором, такі злочини українські ІТ- спеціалісти постійно знаходять та в більшості своїй ліквідують, але слід розуміти, що загроза триває цілодобово. Для вчасної протидії таким злочинам, необхідно використовувати певні інструменти для недопущення таких злочинів. В першу чергу, необхідно мати спеціаліста, який роз'яснює правила поведінки у кіберпросторі в умовах інформаційної війни з рф. Для цього, інструменти має створювати і держава. Мету та роль національної політики у сфері протидії кіберзлочинності розглянемо у наступному розділі.

РОЗДІЛ 2
ІНСТИТУЦІЙНИЙ АСПЕКТ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Мета, завдання та принципи державної політики у сфері протидії кіберзлочинності

Політика держави – це діяльність органів державної влади, спрямована на досягнення певних цілей, таких як вирішення соціальних проблем, реалізація цілей загального значення або розвиток суспільства чи окремих його сфер. Розвиток національного законодавства у сфері кібербезпеки відбувався поступово, з урахуванням міжнародно-правових документів та стратегій кібербезпеки інших країн. Формування та розвиток національної системи заходів протидії кібертероризму в Україні розпочалося у 2011 році з прийняттям Рішення РНБОУ "Про виклики та загрози національній безпеці України у 2011 році", в Указі Президента України № 1119/2010 від 10 грудня 2010 року(наразі не є чинним), за участю СБУ передбачалася підготовка пропозицій щодо створення єдиної національної системи боротьби з кіберзлочинністю та переліку об'єктів, які мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак.

Указ Президента України № 96/2016 від 15.03.2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"" слід розглядати як захід протидії кібертероризму[22]. Метою стратегії кібербезпеки України є створення необхідних умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави. Стратегія спрямована на розвиток спроможностей сектору безпеки і оборони для боротьби з кібертероризмом, протидії кібератакам на електронні інформаційні ресурси держави та об'єкти критичної інфраструктури, протидії розвідувально-підривній діяльності,

спрямованій проти України з боку іноземних спеціальних служб, організацій, груп та окремих осіб у кіберпросторі. Закон передбачає необхідність підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібертероризму [6]. Однак найважливішим нормативно-правовим актом, що закладає основи створення та розвитку національної системи протидії кібертероризму в Україні, є Закон України "Про основні засади забезпечення кібербезпеки України" [19], в якому зазначено, що кібербезпека є важливим для України інтересом людини і громадянина, суспільним, державним та національним інтересом. Він встановлює правові та організаційні засади забезпечення захисту інтересів, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій та інших суб'єктів. Закон є комплексним спеціальним законодавчим актом у сфері кібербезпеки [2, с. 103]. На наступній схемі показано цілі, завдання та принципи державної політики у сфері протидії кіберзлочинності.

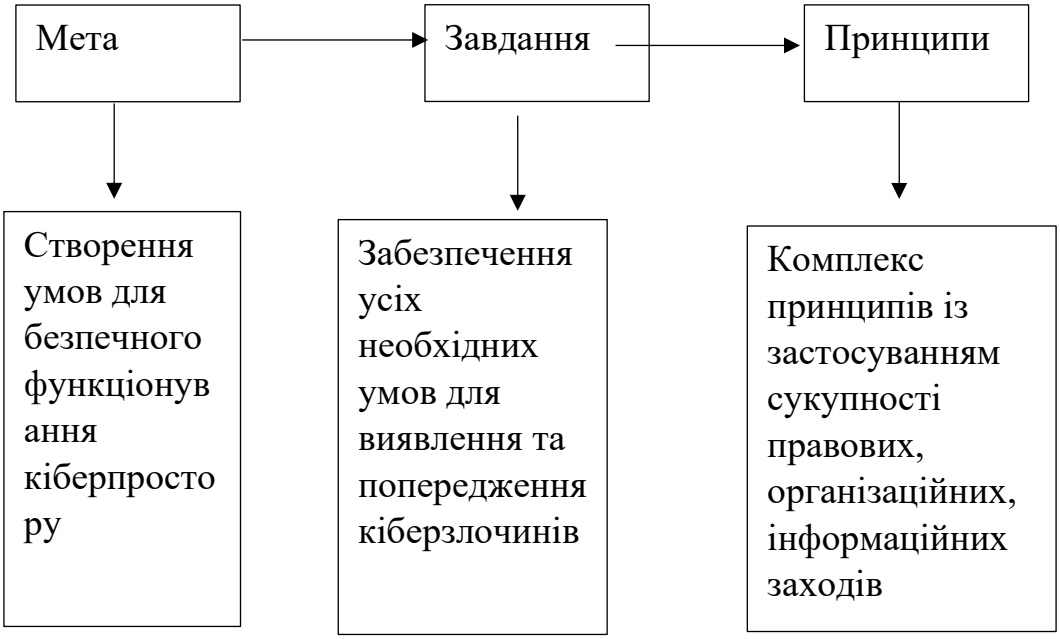


Рисунок 2.1. Сутність мети, завдання та принципів державної політики у сфері протидії кіберзлочинності

Таким чином, цілі національної політики у сфері боротьби з кіберзлочинністю можна підсумувати як створення умов для безпечного

функціонування кіберпростору та ефективного використання кіберпростору на благо окремих осіб, суспільства та країни.

Завданнями національної політики у сфері протидії кіберзлочинності є:

– створення ефективного та доступного контактного центру для повідомлення про випадки кіберзлочинності та шахрайства в кіберпросторі, підвищення ефективності діяльності правоохоронних органів, особливо їх регіональних підрозділів, у протидії кіберзлочинам;

– удосконалення процесуальних механізмів збирання доказів про злочини в електронній формі, удосконалення методів, засобів і прийомів класифікації, ідентифікації та обліку кіберзлочинів, проведення експертних досліджень;

– блокування операторами та провайдерами телекомунікацій окремих (ідентифікованих) інформаційних ресурсів (інформаційних послуг) за рішеннями судів;

– регулювання порядку внесення операторами та постачальниками телекомунікацій обов'язкових розпоряджень щодо аварійного обліку а також зберігання комп'ютерних даних і даних про трафік;

– вирішення питання про можливість екстреного вчинення процесуальних дій в режимі реального часу з використанням електронних документів та електронного цифрового підпису;

– виконання координаційного плану (протоколу) правоохоронних органів протидії кіберзлочинності;

– навчання через свої особливості, для роботи з кримінальними доказами, отриманими в електронному вигляді, необхідні суддя (слідчий суддя), слідчий та прокурор кіберзлочинності;

– підвищення якості персоналу правоохоронних органів.

Реалізація національної політики України у сфері протидії кіберзлочинності як національної політики щодо захисту життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі

шляхом комплексного застосування комплексу правових, організаційних та інформаційних заходів передбачається базується на таких принципах:

– верховенство права та дотримання прав людини, прав і свобод громадян;

– забезпечення національних інтересів України;

– відкритість, доступність, стабільність та безпека кіберпростору;

– державно– приватне партнерство; широка співпраця з громадянським суспільством у сфері кібербезпеки та кіберзахисту;

– пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам

– пріоритетність превентивних заходів;

– необхідність визначити покарання за кіберзлочини;

– пріоритет повинен надаватися розвитку та підтримці науково-технічного та виробничого потенціалу країни;

– зміцнення взаємної довіри у сфері кібербезпеки, вироблення спільних підходів до кіберзагроз, посилення зусиль з розслідування та запобігання кіберзлочинам, а також міжнародне співробітництво з метою запобігання використанню кіберпростору в незаконних та військових цілях;

– Українське законодавство гарантує демократичний цивільний контроль над національними збройними силами та правоохоронними органами, що діють у сфері кібербезпеки, зазначаючи в Стратегії кібербезпеки України, що "розвиток і захист кіберпростору має бути складовою державної політики у сфері впровадження електронного урядування, забезпечення безпеки та сталого функціонування електронних комунікацій і національних електронних інформаційних ресурсів, розвитку інформаційного простору та інформаційної інфраструктури". Відповідно до законодавства України, забезпечення демократичного цивільного контролю над національними збройними силами та правоохоронними органами, що діють у сфері кібербезпеки. ".

З метою забезпечення кібербезпеки та готовності до відбиття відкритих атак у кіберпросторі Україна здійснює різноманітні заходи, спрямовані на реагування на стратегічні, юридичні, політичні, технічні та організаційні питання, пов'язаних із безпечним функціонуванням кіберпростору (рис. 2.2).

Рисунок 2.2. Комплекс реалізованих заходів державою з безпечного функціонування кіберпростору станом на 2023 рік

До завдань ДССЗЗІ входить забезпечення функціонування Української урядової команди реагування на комп'ютерні надзвичайні ситуації (CERT-UA) та оцінка стану захищеності національних інформаційних ресурсів в інформаційно-комунікаційних системах державних органів CERT-UA (Українська урядова команда реагування на комп'ютерні надзвичайні ситуації) – спеціальний підрозділ Адміністрації Державної служби спеціального зв'язку та захисту інформації, спеціальний структурний підрозділ Національного центру кіберзахисту, який діє у складі Агентства. Однак цей орган може займатися лише технічне припинення кібератак. Водночас, правовий статус CERT-UA, як і SCCP, законодавчо не визначений.

2.2. Організаційно-технічна модель забезпечення кібернетичної безпеки України

Постановою Кабінету Міністрів України № 1426 від 29 грудня 2021 року (в рамках Закону) України "Про основні засади забезпечення кібербезпеки України") було затверджено організаційно-технічну модель кібербезпеки України. Окрім державного сектору, над цією моделлю та її імплементацією працювала достатня кількість науковців, таких як Р. Лук'янчук, І. Діордіца, Д. Дубов, В. Бухарєв, Ю. Даник та А. Тарасюк [2–9]. Основною темою їхніх робіт були концептуальні засади міжнародного співробітництва у сфері кібербезпеки за участю України та НАТО. Основна частина їх роботи була присвячена розкриттю пріоритетів національної розвідувальної політики в умовах зовнішньої агресії Росії в міжнародному кіберпросторі. Були визначені напрямки діяльності Росії, спрямовані на посягання на національні розвідувальні ресурси інших країн, у тому числі на підрив наших національних інтересів.

Організаційно– технічна модель кіберзахисту представляє собою дії та заходи з боку держави щодо забезпечення національної системи кібербезпеки, щодо забезпечення протидії кібератак та кіберінцидентів. Дана модель передбачає в собі три рівні інтегрованих інфраструктур кіберзахисту:

1. Організаційно-керівна – основні суб’єкти інтегрованих інфраструктур.

2. Технологічна. Даний рівень передбачає взаємодію техпідрозділів щодо обміну інформації, моніторингу кіберпростору та забезпечення безпеки.

3. Базова. Даний рівень передбачає захист суспільства від кібератак на усіх рівнях.

Для забезпечення таких дій на державному рівні було затверджено організаційну та технічну моделі кіберзахисту:

– покращити функціонування системи кіберзахисту України та посилити координацію між ключовими стейкхолдерами у сфері кібербезпеки;

– зменшення вразливості інформаційно-комунікаційних систем та забезпечення їх кіберстійкості;

– створення необхідних умов для розвитку державно-приватного партнерства у сфері кібербезпеки;

– створення ефективної національної системи реагування на кіберінциденти (включаючи розвиток секторальних груп реагування, синхронізацію та координацію їхніх дій);

– посилення національних спроможностей із забезпечення кібербезпеки в кіберпросторі;

– постійний моніторинг стану кіберзахисту об'єктів критичної інфраструктури;

– забезпечення конфіденційності, цілісності та доступності інформації, а також безпеки комунікаційних і технічних систем.

Впровадження організаційно-технічної моделі забезпечує відповідальність суб'єктів, забезпечення кібербезпеки за виконання своїх конкретних та особливих завдань, особливо в умовах військової агресії з боку Росії.

Затверджена на законодавчому рівні організаційно-технологічна модель кіберзахисту має безперебійно функціонувати. Для цього мають виконуватися такі умови:

1. На основі досвіду наших партнерів (ЄС і НАТО), повинна реалізовуватись державна політика в сфері кіберзахисту.
2. Повинна бути координованість між суб’єктами кіберзахисту.
3. Розвиток систем та сил реагування на кіберзагрози.
4. Розвиток, на основі досвіду минулих досвідів та досвідів іноземних країн, та створення систем управління ризиками в кіберпросторі. По можливості, створювати умови, щоб шахраї не мали змоги реалізувати свої плани.
5. Підвищити взаємодію державних органів та бізнесу в сфері кіберзахисту інформації.

6. З боку держави мають бути створені умови для збільшення кадрового потенціалу в розвитку ІТ та спеціальної, мотивувати молодих спеціалістів залучатися до вирішення питань кіберзлочинів.

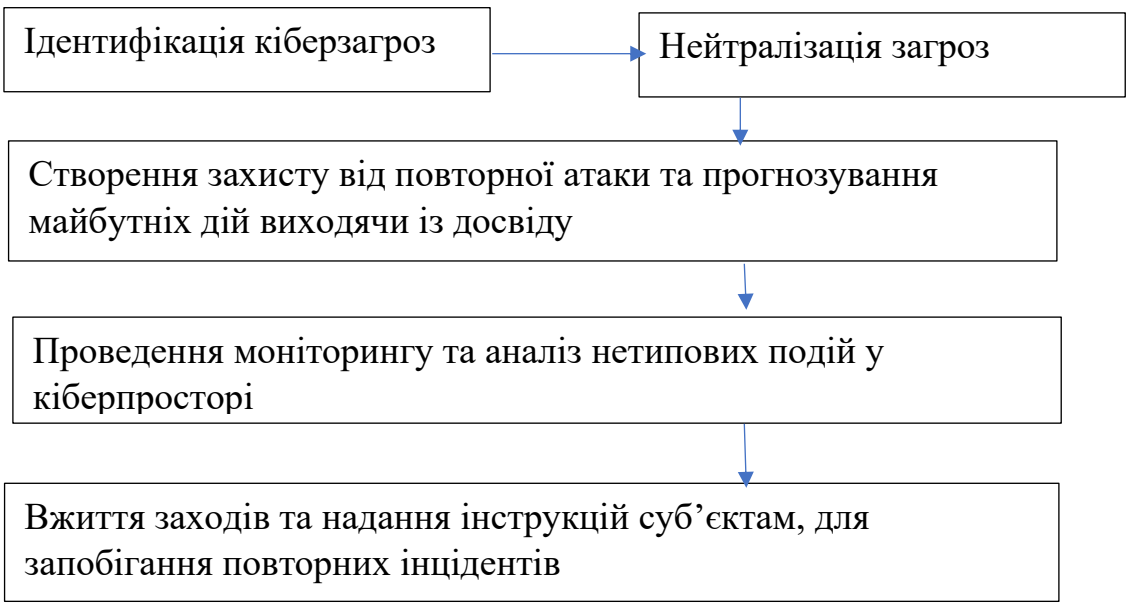
Засоби боротьби в інфопросторі в умовах війни з росією мають бути на сьогодні більш поширеними, адже кібератаки російських хакерів наносять шкоду державі, приватному сектору. В росії створені спеціальні підрозділи для здійснення кібератак на сучасному етапі, таких наприклад як «кіллнет». На початку повномасштабного вторгнення у лютому 2022 року їх атаки мали високу результативність, держава їх фінансує на високому рівні створюючи умови для нанесення шкоди як Україні так і країнам ЄС. На мій погляд, Україна має також створювати умови для захисту кіберпростору і не економити на цьому. Основними засобами для впровадження організаційно-технічної моделі кіберзахисту мають бути:

– Високоякісні системи виявлення кіберінцидентів – інформаційні технології, пристрої, обладнання, програми останніх поколінь.

– Команди реагування – спеціалісти мають проходити постійне підвищення кваліфікації, відстежувати усі можливі варіанти кіберінцидентів у інфопросторі.

– Допомога держави та її захист для приватного сектора [18].

Таким чином, здійснення кіберзахисту має такий алгоритм дій (див. рис.)



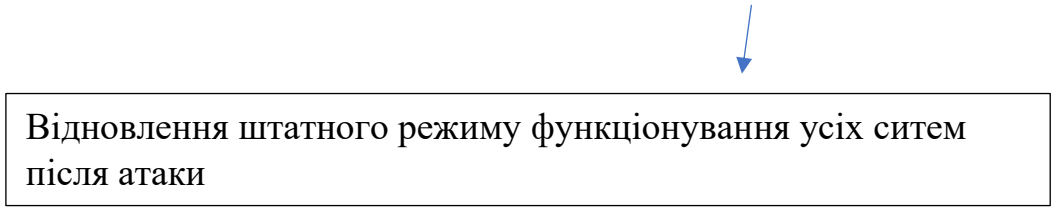


Рисунок 2.3 – Алгоритм дій здійснення заходів щодо кіберзахисту в рамках організаційно– технічної моделі кіберзахисту

Вважаю, що здійснення алгоритму, представленого вище на рисунку, забезпечить функціонування базисної інфраструктури кіберзахисту. Завдяки діям алгоритм буде забезпечений захист національних інфомереж, починаючи від електронних закінчуючи інформаційним, буде забезпечений захист критичної інформаційної інфраструктури, захист громадян. Завдяки таким заходам, формується культура кібербезпеки, починаючи від населення, і закінчуючи державними установами вищого рівня.

Базова інфраструктура кіберзахисту функціонує для забезпечення захисту життєво важливих інтересів особи/людини, суспільства/держави та національних інтересів у кіберпросторі. В додатку надана орієнтовна модель, яка була представлена на конгресі в 2020 році, і яка застосовується задля кіберзахисту України.

2.3. Оцінка та роль кібернетичних атак в інформаційній війні рф проти України

У 2014 році Україна стала жертвою агресивних дій Російської Федерації, яка анексувала Крим, а згодом розв'язала збройний конфлікт у Донецькій та Луганській областях. На офіційному сайті Українського національного інституту пам'яті в історичній довідці про війну зазначається, що "приблизна кількість українських жертв бойових дій оцінюється в 30– 35 тисяч, з них понад 7 тисяч загиблих (цивільні особи та українські військові)" [15]. Приблизно 1,5 мільйона жителів східної України були змушені покинути свої домівки. Інфраструктура на окупованих територіях була зруйнована, а 27% промислового потенціалу Донбасу було незаконно передано Росії, що

доповнює аналіз інформаційної війни між Російською Федерацією та Україною в розвідувальному співтоваристві з 2014 року, до початку повномасштабної війни. 24 лютого 2022 року з раннього ранку президент Росії Путін оголосив про своє рішення провести "спеціальну військову операцію" на території України. Російські війська почали обстріли Києва, Харкова, Одеси, Маріуполя, Дніпра та низки інших міст [5]. Війна тривала вісім років у "гібридному" стані, поки Росія відкрито не напала на Україну близько 5 ранку 24 лютого 2022 року. З моменту проголошення незалежності України з 2014 року ведеться активна інформаційна війна, основними інструментами якої є російські традиційні та електронні засоби масової пропаганди. Найвпливовішими з них є інтернет-телебачення, інтернет-радіо, інтернет-газети, інтернет-журнали та соціальні мережі, які масово поширюють дезінформацію, програмують аудиторію на спотворені повідомлення та контролюють свідомість людей. Російський уряд не лише руйнує Україну, але й фінансує численні видання за кордоном, які впроваджують політику Путіна та дискредитують Україну в цілому в очах міжнародної спільноти. Російська Федерація використовує такі методи інформаційної війни: "інформаційний демпінг" у поєднанні з дезінформацією, з масштабним викривленням подій, припущення, що слугують пропаганді, особисті думки, подання вибіркових фактів, рефреймінг інформації, викривлення інформації та її подання "без коментарів", заборонені міжнародним правом технології "25-го" кадру, замовчування ключових фактів, наприклад, як показано на рисунку 2.4.

Рисунок 2.4. Методи інформаційної війни, які використовує росія проти України

На жаль, обидва ці методи впливають на психіку окремих людей і суспільства в цілому, призводячи до того, що люди сприймають нав'язані ЗМІ думки і переконання як власний життєвий досвід і власні висновки.

Основні наративи антиукраїнської пропаганди в Росії в рамках аналізу інформаційної війни між Російською Федерацією та Україною в інформаційному суспільстві у 2014-2022 роках в медіа. Представлено їх у таблиці 2.1.

Таблиця 2.1

Основні наративи антиукраїнської пропаганди в російських медіа

Антиукраїнська пропаганда, її види в російський медіа	Відсоток згадувань
Свідоме невиконання Мінськ– 1, Мінськ– 2	30,4
Підрив водозабезпечення Україною для Крим	20,6
України – це штучно утворена країна	4,3
Інше (мова, північний потік тощо)	9,7
Втручання у політичні справи Білорусії	13
Фашисти та бандери в Україні	6,5
Дискредитація української влади в особі Зеленського	5,4
Православна церква України – це розкольничество	4,3
Вагнерівці в Білорусі	4,3
Інше	1,5

Для наочності, на наступному рисунку здійснено порівняння, яка пропаганда є найсильнішою.

Рисунок 2.5 – Антиукраїнська пропаганда в російських медіа

Як бачимо з таблиці та рисунку, найбільша пропаганда в російських медіа це те, що Україна не виконувала Мінських угод, тому розпочалась війна.

Контент-аналіз однієї з найпопулярніших пошукових систем Google показує, що ця тема досить активно обговорюється в інформаційному просторі. Запит "інформаційна війна" генерує 8 610 000 (0,62 секунди) посилань, а посилання, пов'язані з фразою "інформаційна війна Російської Федерації проти України" - 4 300 000 (0,54 секунди). Онлайн-ресурс надає щоденні новини про події в Україні. Матеріали на порталі є образливими та перекрученими. Журналісти допускають емоційну лексику щодо України, її уряду, армії та активістів, і заголовки не є винятком. Існують численні так звані "пропагандистські групи". Це особливо помітно на таких новинних порталах, як "Правда.ру" та "Московский комсомолец", де добре відомі навішування ярликів, апеляція до авторитетів, демонізація ворога, спрощення фактів, щоденні наративи, емоційний резонанс та анонімні авторитети, ігри з "приписуванням" росіянам, "спільною думкою" та ін. Було виявлено, що використовувалися добре відомі пропагандистські методи. Ці методи викликають почуття приналежності до "великої і могутньої" Росії та її "братнього народу". У такий спосіб автори матеріалів нав'язують суспільству певні цінності, ідеї та програми.

Інформаційні вкидання здійснюють ІТ-фахівці: за даними Google, навіть у січні- квітні 2022 року кібератаки на український уряд, військові організації та ІТ-ресурси критичної інфраструктури були більш руйнівними, ніж за попередні вісім років. І важливо зазначити, що пік хакерської активності припав на початок повномасштабного вторгнення Росії в Україну.

Ці російські кібероперації мають три основні цілі:

- Підірвати діяльність українського уряду.
- Припинити міжнародну підтримку українського уряду.
- Підтримати військове вторгнення Росії на територію України.

В наступній таблиці показано, які види кібератак наразі існують, і на які галузі йде найбільший потік кібератак.

Таблиця 2.2

Галузі, які зазнають найбільших кібератак з початку вторгнення рф

Кібератаки рф по галузям	Відсоток кібератак
Фінанси	5
Телекомунікації	7
Транспортна галузь	7
Енергетика	8
Медіа	9
ІТ– галузь	10
Держоргани	27
Інші	27

Для наочності, представимо дану інформацію у вигляді рисунку. На рисунку видно, що найбільші кібератаки зазнають державні органи та ІТ-галузь. Кібератаки спрямовані на пониження значення державних органів а ІТ -галузь для її ослаблення при виявленні зовнішніх загроз.

Рисунок 2.6 – Відсоток кібератак рф проти України з початку вторгнення

Щодня кількість кібератак зростає, а їхні структури стають складнішими. Наприклад, Державна служба спеціального зв'язку заявила, що лише у грудні 2023 року відбила майже 400 потужних DDoS– атак, зафіксувавши понад 170 000 спроб використання вразливостей, тисячі заражень та сотні сканувань. Тому показово, що у 2022 році Україна посіла друге місце у світі після США за кількістю кібератак на країну. [15]

З вказаного вище, у другому розділі роботи, робимо такі висновки. Державна політика відіграє важливу роль у сфері протидії кіберзлочинності. На державному рівні значно легше реалізовувати в дію проекти задля забезпечення безпеки в кіберпросторі. Метою державної політики в сфері протидії кіберзлочинності є створення умов для реалізації заходів захисту кіберпростору. Завдання, які має виконувати і виконує державна політика в сфері протидії кіберзлочинності – забезпечення усіх необхідних умов для виявлення та попередження кіберзлочинів. Комплекс принципів має складатися із сукупності правових, організаційних, інформаційних заходів.

Задля цього, в грудні 2021 році вийшла Постанова Кабінету міністрів про організаційно-технічну модель забезпечення кібернетичної безпеки України. Основними тезами даної моделі є - забезпечення всіх умов та заходів задля кіберзахисту в інфопросторі, як державних структур так приватного сектору і населення. Особливого значення ця модель та її реалізація набули в умовах широкомасштабної агресії росії проти України. Реалізація моделі передбачає ефективність від виявлення, нейтралізації та захисту

кіберінцидентів. Дана модель має свою ефективність дивлячись на оцінку та роль кібернетичних атак в інформаційному просторі з боку рф. Якщо в перші дні військової агресії інфопростір був в російській пропаганді, то зараз ми спостерігаємо зворотній ефект. Отже, на мою думку, організаційно-технічна модель кіберзахисту працює та захищає від невірної інформації в мережах інфопростору.

РОЗДІЛ 3
МЕХАНІЗМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ КІБЕРЗАГРОЗАМ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

3.1. Проблеми та перспективи вдосконалення державної політики у сфері протидії кіберзлочинності в Україні

Нормативно-правова база України у сфері кіберзлочинності має ряд протиріч, що суттєво заважає в ефективній боротьбі проти такого роду злочинів. Проблеми забезпечення кібербезпеки вирішуються прийняттям Законів України та нормативних документів, що охоплюють регулювання кібербезпеки держави. На сьогодні діючими є такі правові та концептуальні засади:

1. Закон України "Про основні засади забезпечення кібербезпеки України".

2. Постанова Кабінету Міністрів України "Про затвердження загальних вимог щодо забезпечення кіберзахисту об'єктів критичної інфраструктури".

3. Закон України "Про інформацію".

4. Закон України "Про захист інформації в інформаційно–комунікаційних системах".

5. Закон України "Про державну таємницю".

6. Закон України "Про електронні документи та електронний документообіг".

7. Доктрина інформаційної безпеки.

8. Закон України "Про національну безпеку України".

9. Стаття 15 Кримінального кодексу України. Контроль за законністю заходів кібербезпеки в Україні, тощо.

Невідповідність термінів в законодавчих актах ускладнює нейтралізацію та понесення відповідальності за здійснене в правовому полі. Так у Законі України «Про національну безпеку України» використовуються

терміни «комп'ютерна злочинність» та «комп'ютерний тероризм». Проблема полягає у тому, що ані в вищезгаданому документі, ані в інших нормативних актах не має чіткого визначення цих термінів. Навіть якщо вдатися до тексту Закону України «Про боротьбу з тероризмом» , ми не побачимо взагалі визначення «комп'ютерний тероризм».[5] В «Доктрині інформаційної безпеки України» також згадуються вищезазначені терміни, але й там немає чіткого визначення. Відсутність пояснень чи посилань призводить до непорозумінь та створює невідповідність кіберзлочинів як таких. Також в Доктрині згадується «кібератака» , але тлумачення даного терміну немає. На мою думку, такий стан речей свідчить про те, що вітчизняна нормативно-правова база використовує в своїй діяльності терміни, яких по суті немає [23].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та документи, що супроводжують цей документ мають застарілу інформацію і не відповідають сучасності. Адже усім відомо, що ІТ- прогрес не стоїть на місці, а розвивається семимильними кроками. Згідно цього Закону, на державних підприємствах, у приватних компаніях інтернет-провайдери мають застосовувати Комплексну систему захисту інформації , яка вже є багато років неефективної та крім цього, вже й застаріла.

Вважаю, з вищевикладеного, таке становище речей призводить до проблем координації діяльності правових структур та нейтралізації злочинів на правовому рівні, що впливає на комплекс процедур з протидії кіберзлочинів та їх попередження.

Наступною, на мій погляд, проблемою державної політики в сфері кібербезпеки є неефективна робота системи кіберрозвідки. Адже, існують приклади, коли приватний сектор попереджував державні органи про зовнішні кібератаки. В умовах війни кіберрозвідка повинна бути на високому державному рівні.

Основними перспективами державної політики в сфері кіберзахисту є визначення ключових принципів та напрямків для покращення кібербезпеки в

Україні. Основна ідея – дозволити приватному сектору процес саморегуляції, тобто самостійно виявляти та визначати стандарти кібербезпеки суто для тієї галузі, яка цього потребує. В даному випадку, держава буде виступати не як регулятор, а як вищий орган у допомозі вирішення проблем кібербезпеки на законодавчому рівні.

Таким чином, з вказаного вище можна узагальнити проблеми державної політики в сфері кіберзахисту:

1. Протиріччя визначення термінів в законодавчих актах;
2. Відсутність тлумачень щодо державних структур, які вирішують питання кібератак;
3. Застарілі системи захисту від інтернет– провайдерів, які підпорядковані державі.

Виходячи з аналізу основних проблем, вважаю, що перспективи державної політики в сфері безпеки є досить глобальні за дотриманням таких вимог:

1. Вдосконалити нормативну правову базу;
2. Оновити систему захисту;
3. Дозволити приватному сектору самостійно регулювати свій кіберзахист і запровадити галузеві стандарти кібербезпеки;
4. Для мінімізації збитків від кібератак потрібно не лише захищати алей правильно передбачати інциденти кібератак;
5. Важливим елементом є формування культури кібербезпеки у суспільстві. Правила кібергігієни мають закладені дітям ще в початкових класах;
6. Мотивувати молодь отримувати спеціальність в ІТ– галузях з боку саме держави.

В умовах російської агресії держава має особливо вплинути на подолання проблем в кібербезпеці, адже від цього залежить її суверенітет.

3.2. Роль міжнародного середовища у протидії кіберзлочинності в Україні

Міжнародне середовище відіграє важливу роль у протидії кіберзлочинності в Україні. Основними партнерами України є Європейський Союз (далі ЄС) та Сполучені штати Америки (далі США).

Загальні положення про кібербезпеку ЄС викладені в таких документах:

- Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційно–комунікаційних технологій і скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку).
- Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи щодо забезпечення високого рівня безпеки спільних мереж та інформаційних систем в ЄС.
- Рекомендація Комісії (ЄС) 2017/1584 від 13 вересня 2017 року про скоординоване реагування на великі інциденти та кризи у сфері кібербезпеки.
- Рекомендація Комісії (ЄС) 2019/534 від 26 березня 2019 року про кібербезпеку в мережах 5G.
- Стійкість, стримування та оборона: Розбудова стійкої кібербезпеки для ЄС.
- Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року про обробку персональних даних і захист приватності у сфері електронних комунікацій (Директива про захист приватності та електронні комунікації).
- Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та про

скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

- Послання Європейського Парламенту та Комісії щодо сприяння захисту даних за допомогою технологій, що підвищують рівень приватності.
- Стратегія кібербезпеки ЄС: відкритий, безпечний і надійний кіберпростір.
- Зміцнення європейської системи кіберстійкості та розвиток конкурентоспроможної та інноваційної індустрії кібербезпеки.
- Конвенція про кіберзлочинність 2001.XI.23
- У США кібербезпека регулюється наступними законодавчими актами
- Закон про обмін інформацією з питань кібербезпеки від 2015 року.
- Закон про переносимість, доступність та підзвітність медичного страхування (1996 р.).
- Закон про фінансову модернізацію 1999 року (Закон Грамма– Ліча– Блайлі).
- Закон про національну безпеку 2002 року.
- NIST (Національний інститут стандартів і технологій) Спеціальна публікація 800– 82 – Посібник з безпеки промислових систем управління.
- NIST SP 800– 50 – Створення програми підвищення обізнаності про IT– безпеку.
- NIST SP 800– 40 – Посібник з методів управління вразливостями.
- NIST 800– 53 – Управління безпекою та конфіденційністю для федеральних інформаційних систем та агентств.
- NIST 800– 53 – Рекомендації з цифрової ідентифікації.
- Взаємодія євроатлантичного і євразійського просторів в сфері кібербезпеки набуває важливого значення в створенні загальних

безпекових інститутів таких як ООН, ОБСЄ, НАТО, ЄС, РЄ. Ці органи працюють разом, щоб охопити якомога ширший спектр питань безпеки та уникнути дублювання функцій. ООН відіграє особливу роль у вирішенні питань міжнародного співробітництва в боротьбі з кіберзлочинністю і постійно обговорює питання запобігання та боротьби з комп'ютерними злочинами.

Роль ОБСЄ І НАТО полягає в регулюванні та попередженнях конфліктів, недопущення кризового становища, а також реагування на безпекові виклики. ОБСЄ виступає регулятором в обговоренні питань світового рівня які є важливими для загальної безпеки. Країни-члени НАТО та ОБСЄ обмінюються інформацією з питань кібербезпеки у тому числі. Тісна співпраця між НАТО, ЄС і ОБСЄ є одним з елементів "комплексного підходу" до врегулювання криз, який вимагає ефективного використання як військових, так і цивільних інструментів [18].

На підставі ст. 14 Закону України «Про основні засади кібербезпеки в Україні» регламентовано такі засади міжнародного співробітництва:

1. Україна відповідно до укладених міжнародних договорів здійснює співпрацю з іноземними державами;
2. Україна, відповідно до міжнародних договорів, може приймати участь у спільних міжнародних заходах з обговорення питань захисту в сфері кібербезпеки в рамках дозволеного з боку Верховної ради України;
3. Відповідно да законодавства України, держава може приймати участь в міжнародній співпраці з іноземними державами в рамках своїх повноважень;
4. На підставі запиту з боку міжнародного співтовариства надавати інформацію щодо кібербезпеки державам, які цього потребують.

Для реалізації таких заходів важливо вивчити міжнародний досвід міжнародних організацій у цій сфері, вжиті ними заходи та ефективність їх впровадження.

Держави-члени НАТО акцентують увагу на налагодженні сталого діалогу між країнами та запровадження дієвих механізмів протидії викликами, якими супроводжується їх діяльність у кіберпросторі. Відкрита інформаційна сфера, відповідальна поведінка держав в сфері кібербезпеки, довіра в обміні інформацією, заходи нарощування потенціалу безпеки в кіберпросторі – це пріоритетні напрямки країн НАТО.

3.3. Виклики глобальній кібернетичній безпеці як наслідок інформаційної війни рф проти України та шляхи їх подолання

З початком повномасштабної війни рф проти України, світ розділився. Крім військових дій на території України існує ще інформаційна війна рф не тільки в Україні а й по всьому світі. Тому, на мою думку, дана проблема не є суто внутрішньодержавною. Кіберудари та інформаційна політика рф зумовлює світ глобально дивитись на подолання кібернетичної загрози. Як можна бачити з новин, більшість країн не підтримують рф, але існують й такі, що на її боці або відсторонилися від конфлікту. Як приклад глобальної загрози в інформаційній війні може бути ситуація з Запорізькою АЕС. Станом на сьогодні інфопростір заповнений пропагандою про загрозу АЄС. Якщо щось станеться на атомній електростанції, увесь світ це відчує і, звичайно всі віддають собі звіт про можливі наслідки. Як стало відомо, на Запорізьку АЕС російські окупанти завезли 14 журналістів – пропагандистів. Як стверджує інформаційне агенство UNIAN: "Найближчим часом вони опублікують багато нісенітниць про "безпеку" найбільшого в Європі ядерного об'єкта, щоб "переконливо" виправдати ядерний тероризм окупантів". Також планується зняти сюжети про те, як працівники АЕС дякують "асбабадівцям" (звісно, під дулами автоматів), заспокійливі мантри про експертний менеджмент "Росатому" та готовність приймати делегації МАГАТЕ, "благодійний" дозвіл на продовження виробництва електроенергії для потреб України та інші

махінації[38]. Такий приклад інформаційної війни дестабілізує населення не лише України а й населення країн-сусідів.

Задля вирішення глобальних викликів з боку рф, найбільш пріоритетний партнер – США, за результатами кібердіалогів надає Україні фінансування на розвиток проектів з посилення кібербезпек, а також для підготовки кіберфахівців.

Технології розвиваються, а отже такі операції стають дедалі складнішими. Ми спостерігаємо, як інструменти, що використовуються під час традиційних кібератак, застосовуються державними органами в операціях із кібервпливу на додачу до посиленої координації та розповсюдження. Операції з кібервпливу на іноземні країни складаються з трьох етапів: підготовка, поява дезінформації та її розповсюдження. На наступному рисунку розглянемо процес розповсюдження дезінформації у глобальному просторі.

Рисунок 3.1. Наочний приклад поширення дезінформації в межах трьох основних етапів операції з кібервпливу на іноземні країни [13]

До цих етапів належать підготовка, поява дезінформації та її розповсюдження.

На цій схемі показано три етапи операції з кібервпливу на іноземні країни: підготовка (прес- конференція), поява дезінформації (висвітлення події в російських ЗМІ) й розповсюдження (в іноземних виданнях).

Відстеження індексу результативності російської пропаганди показує, що станом на березень 2023 року майже 1000 американських веб-сторінок

посилалися на інформацію з російських пропагандистських сайтів. Найпоширенішими темами були війна в Україні та внутрішня політика США.

Індекс результативності російської пропаганди відстежує потік новин від російських державних і спонсорованих ЗМІ й видань, які їх розповсюджують як частину загального новинного трафіку в Інтернеті.

Індекс результативності російської пропаганди в США з жовтня 2022 року по квітень 2023 року показує, наскільки підвищився її рівень із моменту повномасштабного вторгнення Росії в Україну 24 лютого 2022 року.

Для того, щоб боротися із кіберзлочинами в інформаційному просторі існують такі шляхи подолання.

Глобальна кібербезпека мусить спрямовувати зусилля на захист та безпеку мережі з використанням наступних рівнів захисту інформації:

1) Попередження – вхід в базу даних та технологій надається лише уповноваженому персоналу з відповідними спеціальними навичками;
2) Виявлення – забезпечити раннє виявлення злочинів та зловживань, навіть якщо існують механізми захисту;
3) Стримування – зменшує розмір збитків, якщо правопорушення вчиняються, не дивлячись на запобігання та виявлення; та
4) Відновлення – забезпечує суттєво нові дані за наявності задокументованого та протестованого плану відновлення" [23].

Реалізація цих заходів вимагає більших інвестицій у кібербезпеку для запобігання атакам на великі компанії в державному та приватному секторах, а також для протидії намірам дестабілізувати суспільство. Крім того, для того, щоб будь-яке суспільство відчувало себе принаймні юридично захищеним у кіберпросторі, необхідні письмові правила, стандарти, норми та інструкції. Наразі з'являються галузеві нормативні акти щодо кіберризиків, а законодавчі органи виявляють дедалі більший інтерес до цієї сфери. Україна перебуває в процесі розробки стандартів безпеки для об'єктів критичної інфраструктури. Зростає заклик до більш активного обміну інформацією та обов'язкового

інформування про кібератаки з метою спільної боротьби з кібератаками та мінімізації їхніх наслідків. Залишається сподіватися, що обов'язкові вимоги в цій сфері будуть встановлені. Якщо, з якихось причин, цього не буде в найближчому майбутньому, загальна атмосфера сьогодні така, що регулятори, державні органи тощо хочуть підвищити свої знання з кібербезпеки. Тому українські ІТ-спеціалісти повинні шукати можливості для взаємодії зі своїми колегами з метою обміну знаннями та з іншими зацікавленими сторонами задля покращення ситуації з кібербезпекою в країні.

На мою думку, наразі гібридна війна ведеться з використанням кіберзброї, технології постійно вдосконалюються, що призводить до її модернізації, а кіберінциденти часто мають значний вплив як на окремих осіб, так і на економічну, промислову та національну безпеку. Тому питання кібербезпеки набувають все більшого значення в усьому світі, а для України – ще більшого. У порівнянні з 2014 роком, кіберфронт України зміцнився. Глобальний індекс кібербезпеки (GCI), складений Міжнародним союзом електрозв'язку, зріс майже вдвічі – з 0,353 до 0,661. Однак, за класифікацією МСЕ, Україна залишається на середньому рівні. Це означає, що вона належить до країн, які активно зміцнюють сектор кібербезпеки та беруть участь у відповідних програмах та ініціативах. Рух України до безпечного кіберсередовища підтверджується, зокрема, партнерством з Північноатлантичним альянсом та окремими країнами. Однак брак фінансування залишається найбільшою перешкодою для цього розвитку" [38].

Отже, з вказаного вище робимо висновок. Державна політика в сфері кібербезпеки має ряд проблем. Основні з них стосуються законодавчої бази – а саме невідповідність або відсутність визначення термінів щодо кібербезпеки, що створює проблеми в регулюванні таких злочинів в правовому полі. Також важливою проблемою є відсутність прогресу з боку держави в системах захисту в кіберпросторі, відсутність співпраці між державою та приватним сектором в вищезазначеній сфері. Досить важливим елементом відсутності прогресивного розвитку – є відсутність ініціативи з боку держави створювати

високо кваліфікаційні кадри в сфері ІТ. Освіта здійснюється за гроші і, відповідно існує ймовірність відтоку кадрів за кордон. Перспективи вдосконаленні висвітлюються з боку вирішення проблем. Якщо всі вище згадані проблеми будуть вирішені, то і перспективи кібербезпеки в Україні будуть на високому рівні. Роль міжнародного середовища в протидії кіберзлочинності регулюється Законами України та в рамках її повноважень. На сьогодні, законодавство України передбачає можливість участі та співпраці з іноземними країнами в сфері кібербезпеки. Основними міжнародними інститутами, що регулюють стан кібербезпеки у світі є ООН, ОБСЄ, НАТО, ЄС тощо. У мовах військової агресії з боку рф та інформаційної війни в інфопросторі, виникли глобальні виклики кібернетичній безпеці не лише для України а й для інших країн. Держава-агресор вкладає кошти в розвиток ІТ–спеціалістів, що можна було побачити на початку 2022 року в результатах діяльності «кіллнет», але міжнародне середовище згуртувалось та намагається не допустити інформаційної війни в кіберпросторі.

ВИСНОВКИ

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати його національні інтереси розглядається як важлива складова кібербезпеки. Кількість кібератак та кінетичної зброї як проти військових, так і проти цивільних цілей не є чимось новітнім, але їх кількість та використання проти критичної інфраструктури викликає тривогу. Хоча вони не відіграють великої ролі в тактичних досягненнях жодної зі сторін, але в будь-якому випадку використовуються як засіб руйнування, підриву та озброєння даних, а також як засіб поширення дезінформації та пропаганди[22].

Таким чином, відповідно до мети були вирішені наступні завдання:

1. В роботі було представлено теоретико-методологічний аналіз терміну "кіберзлочинність". Термін "кіберзлочинність" не має чіткого визначення в жодному нормативно-правовому документі. Термін "кіберзлочинність" часто вживається у поєднанні з терміном "комп'ютерна злочинність", і часто ці терміни використовуються як синоніми. Термін "кіберзлочинність" ширший за термін "комп'ютерна злочинність" і точніше відображає природу таких явищ, як злочинність в інформаційній сфері. Кіберзлочинність охоплює як комп'ютерні мережі, так і злочини, скоєні в телекомунікаційній, банківській та інших сферах.

2. Визначення методів і типів кіберзлочинності. Типові приклади кіберзлочинності включають кардінг, фішинг, вішинг, онлайн-шахрайство, хакерство, спільне використання карток, соціальну інженерію, молверінг, незаконний контент і рефайлінг.

3. Проаналізовано засоби боротьби з кіберзлочинністю в умовах інформаційної війни. Існує три напрямки боротьби з кіберзлочинністю: загально соціальні контрзаходи, специфічні кримінологічні контрзаходи та індивідуальні контрзаходи.

Протидія (напрям) кіберзлочинності на загально соціальному рівні включає комплекс перспективних соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на розв'язання актуальних соціальних проблем і протиріч у державі. Саме реалізація загально соціальних запобіжних заходів здатна усунути або мінімізувати дію криміногенних факторів, що детермінують кіберзлочинність та гальмують розвиток особистості правопорушників.

Розробка відповідних заходів протидії злочинності, в тому числі кіберзлочинності, вимагає належного регулювання діяльності як правоохоронних органів, так і вищих органів державної влади, що відповідає вимогам правової, незалежної та демократичної держави. Також необхідно усунути фактори, що сприяють існуванню та розвитку злочинності.

4. Визначено цілі, завдання та принципи державної політики у сфері протидії кіберзлочинності. Участь держави у боротьбі з кіберзлочинністю відіграє важливу роль. Державна політика – це діяльність органу державної влади, спрямована на досягнення певної мети, а саме розв'язання суспільної проблеми, досягнення важливої мети в цілому, розвиток суспільства або його частини. Метою державної політики є забезпечення необхідних умов для розвитку заходів кібербезпеки; завданням державної політики є створення необхідних умов для протидії кіберзагрозам, принципами якої є правові, інституційні та соціальні.

5.Основними інструментами забезпечення кібербезпеки є організаційна та технічна моделі. Розглянуто організаційно-технічну модель забезпечення кібербезпеки в Україні. Організаційно-технічна модель забезпечення кібербезпеки включає інституційну, адміністративну, технічну та базову інфраструктуру кібербезпеки, що реалізується для забезпечення функціонування національної системи кібербезпеки.

6. Оцінка та визначення ролі кібератак в інформаційній війні Росії проти України. Все це необхідно для того, щоб кібератаки не були спрямовані на суспільство і не дестабілізували життя пересічних громадян. Опитування та

аналізи показують, що більшість громадян вірять дезінформації, яка надходить з Росії. ЗМІ є потужним інструментом цілеспрямованого встановлення політичного порядку та засобом налагодження владою необхідних контактів і зв'язків з громадськістю. Тому, як прояв інформаційної війни, вони можуть маніпулювати людьми та формувати громадську думку через ЗМІ. В роботі було розглянуто вплив дезінформації та визначено галузі, які зазнають найбільших кібератак. Проте, українські спеціалісти вже за півтора року повномасштабної війни з рф навчилися гальмувати вплив інформації на українців та спростовувати російські фейки на українському інфопросторі.

7. Визначено проблеми та перспективи вдосконалення державної політики у сфері протидії кіберзлочинності в Україні. Основні з них стосуються законодавчої бази, а саме невідповідність або відсутність визначення термінів щодо кібербезпеки, що створює проблеми в регулюванні таких злочинів в правовому полі. Також важливою проблемою є відсутність прогресу з боку держави в системах захисту в кіберпросторі, відсутність співпраці між державою та приватним сектором в вищезазначеній сфері. Досить важливим елементом відсутності прогресивного розвитку є відсутність ініціативи з боку держави створювати високо кваліфікаційні кадри в сфері ІТ. Освіта здійснюється за гроші і, відповідно існує ймовірність відтоку кадрів за кордон. Перспективи вдосконаленні висвітлюються з боку вирішення проблем. Якщо всі вище згадані проблеми будуть вирішені, то і перспективи кібербезпеки в Україні будуть на високому рівні. Роль міжнародного середовища в протидії кіберзлочинності регулюється Законами України та в рамках її повноважень.

8. Проаналізована роль міжнародного середовища у протидії кіберзлочинності в Україні. Основними міжнародними інститутами, що регулюють стан кібербезпеки у світі є ООН, ОБСЄ, НАТО, ЄС тощо. У мовах військової агресії з боку рф та інформаційної війни в інфопросторі, виникли глобальні виклики кібернетичній безпеці не лише для України а й для інших країн.

9. Розглянуто виклики глобальній кібернетичній безпеці як наслідок інформаційної війни рф проти України та шляхи її подолання. Держава-агресор вкладає кошти в розвиток ІТ- спеціалістів, що можна було побачити на початку 2022 року в результатах діяльності «кіллнет», але міжнародне середовище згуртувалось та намагається не допустити інформаційної війни в кіберпросторі. Шляхи подолання інформаційної війни рф проти України – це створення потужного кіберзахисту на державному рівні та у всіх галузях, починаючи з державних органів та закінчуючи приватним сектором та населенням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азарова Д.С. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно– правові аспекти. Протидія терористичній діяльності: міжнародний досвід і його актуальність для України. Київ, 2018. С. 135–138.
2. Вехов В. Б. Комп'ютерні злочини: способи здійснення та розкриття. : Право и закон, Київ, 2022. 182 с.
3. Державно– приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. URL: https://niss.gov.ua/publikacii/analitichni– dopovidi/derzhavno– privatne– partnerstvo– u– sferi– kiberbezpeki– mizhnarodniy– 0. (дата звернення: 02.06.2023).
4. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ, 2017. 107 с.
5. Доронін І. М. Правові проблеми визначення компетенції суб'єктів забезпечення кібербезпеки України. Актуальні проблеми управління інформаційною безпекою держави Київ, 2018. С. 62–64. URL: http://academy.ssu.gov.ua/upload/file. (дата звернення: 02.05.2023).
6. Закон України «Про боротьбу з тероризмом» № 2997– IX від 21.03.2023. URL:https://zakon.rada.gov.ua/laws/show/638– 15#Text. (дата звернення: 12.05.2023).
7. Закон України «Про основні засади забезпечення кібербезпеки України» № 2470– IX від 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163– 19#Text. (дата звернення: 14.05.2023).
8. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 2849– IX від 13.12.2022 URL:

https://zakon.rada.gov.ua/laws/show/3475– 15#Text. (дата звернення: 12.05.2023).

9. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2022. С. 172–177.
10. Інформаційна війна в Україні і світі: що треба знати. URL: https://gwaramedia.com. (дата звернення: 17.05.2023).
11. Інформаційні виклики для України у другий рік війни. URL: https://www.ukrinform.ua/rubric– polytics/3674668– informacijni– vikliki– dla– ukraini– u– drugij– rik– vijni.html. (дата звернення: 05.06.2023).
12. Інформаційна війна: 5 прийомів пропаганди, до якої вдається путінізм. URL: https://www.ukrinform.ua/rubric– society/3628987– informacijna– vijna– 5– prijomiv– bojovoi– propagandi– do– akih– vdaetsa– putinizm– sob– manipuluvati– ludmi.html. (дата звернення: 10.05.2023).
13. Кібербезпека в умовах війни: представники ДДУВС обговорювали новації та перспективи розвитку сфери. URL: https://dduvs.in.ua/2023/02/21/kiberbezpeka– v– umovah– vijny– predstavnyky– dduvs– obgovoryuvaly– novatsiyi– ta– perspektyvy– rozvytku– sfery. (дата звернення: 12.05.2023).
14. Кібербезпека під час війни: як захистити інформацію та пристрої. URL: https://kyivcity.gov.ua/bezpeka_ta_pravoporiadok/kiberbezpeka_pid_chas_viyni_yak_zakhistiti_informatsiyu_ta_pristro/. (дата звернення: 12.05.2023).
15. Кібербезпека в Україні: шляхи розвитку та можливості. URL: https://www.ukrinform.ua/rubric– technology/3704093– kiberbezpeka– v– ukraini– slahi– rozvitku– ta– mozlivosti.html. (дата звернення: 02.06.2023).
16. Книженко О. О. Сучасний стан злочинів у сфері використання електронно– обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку в Україні. Київ. С. 122–127.

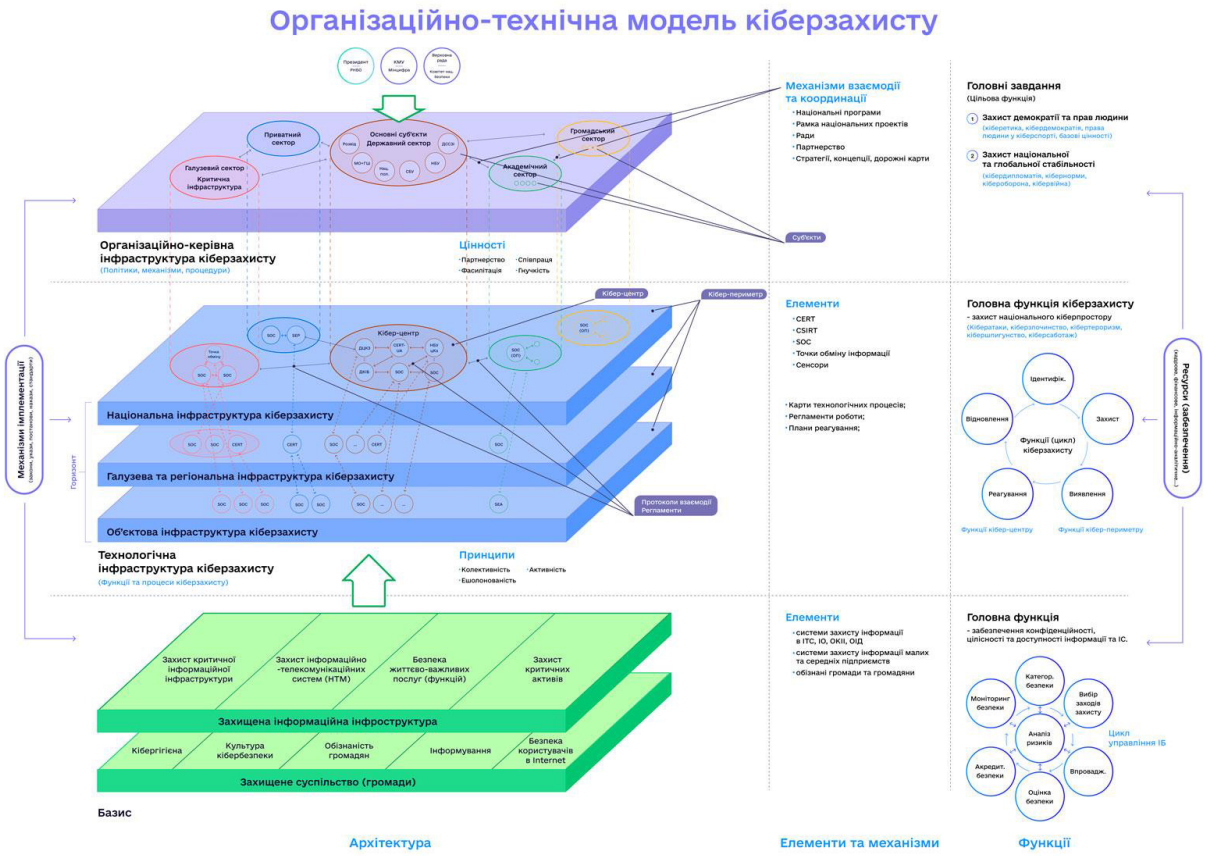
17. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Policy Paper). USAID. 2022. 28 с.
18. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575. (дата звернення: 09.05.2023).
19. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2021. 212 с.
20. Кравцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. URL: http://lsej.org.ua/5_2014/5_2014.pdf. (дата звернення: 08.05.2023).
21. Кримінологія. Академічний курс / кол. авт. ; за заг. ред. О. М. Литвинова. Київ : Кондор, 2021. 588 с.
22. Лавник А.М. Державна політика протидії кіберзлочинності в умовах інформаційної війни рф проти України // XXIII Міжнародна науково– практична конференція здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки». 2023. 106 с. URL: http://fmv.nau.edu.ua/polit/polit– 2023/
23. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю.Є. Максименко, В. М. Желіховський. –Київ : КНТ, 2020. 280 с.
24. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети / Вісник Національної академії державного управління при Президентові України. Серія : Державне управління. – 2022. С. 50– 56.
25. Манжай О. В. Використання кіберпростору в оперативно– розшуковій діяльності. Право і Безпека. 2019. С. 215–219.
26. Максименко Ю. Є. Теоретико– правові засади забезпечення інформаційної безпеки України : монографія / відп. Ред. Ю.Є. Максименко, Київ, 2021. 20 с.

27. Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер– технологій. URL: https://www.rnbo.gov.ua/ua/Diialnist/4658.html. (дата звернення: 10.05.2023).
28. Окупанти завезли на Запорізьку АЕС журналістів– пропагандистів для зйомки фейкового відео. URL: https://www.unian.ua/war/okupanti– zavezli– na– zaporizku– aes. (дата звернення: 02.06.2023).
29. Про Національний координаційний центр кібербезпеки. URL: https://zakon. rada.gov.ua/laws/show/242/2016#Text. (дата звернення: 11.05.2023).
30. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163– VIII. URL: https://zakon.rada.gov.ua/laws/ main/2163– 19#Text. (дата звернення: 11.05.2023).
31. Про ратифікацію Конвенції Ради Європи про кіберзлочинність: Закон України від 07.09.2005 р. № 2824– IV. URL: https://zakon.rada.gov.ua/laws/ show/2824– 15#Text. (дата звернення: 11.05.2023).
32. Постанова «Про затвердження Положення про організаційно– технічну модель кіберзахисту» від 29 грудня 2021 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426– 2021– %D0%BF#Text. (дата звернення: 14.05.2023).
33. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 12.05.2023).
34. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» № 685/2021 від 28.12.2021. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text. (дата звернення 12.05.2023).

35. Петр Г. Прокуратура та правоохоронні органи України в період злочинного режиму Януковича і її перетворення сьогодні. URL: http://www.3republic.org.ua/ua/ideas/13397. (дата звернення: 08.05.2023).
36. Потерейко О. О. Віртуалізація держави: теоретико– методологічний аналіз : Львів, 2021. 201 с.
37. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : зб. наук. пр. Київ : Вид.– поліграф. центр «Київ. ун– т», 2019. Вип. 19. С. 338–342.
38. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів / Руслан Юрійович Сень // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали між– нар. наук.– практ. конф., Харків : Права людини, 2021. С.192–194.
39. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю / Харків. нац. ун– т внутр. справ. –Харків : Права людини, 2022. С.194–196.
40. Сідак В. С.Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С.Сідак, В.Ю. Артемов. –Київ : КНТ, 2007. 160 с.

ДОДАТКИ

Додаток 1



Модель складатиметься з трьох вертикально та горизонтально інтегрованих інфраструктур. «Перший рівень – це організаційно– керуюча інфраструктура кіберзахисту. Складовими елементами цієї інфраструктури є суб'єкти національної системи кібербезпеки, які визначені відповідним законодавством на цей час. Суб'єкти кіберзахисту згруповані у державний, академічний, приватний, громадський та регіональний сектори.

Другий рівень – це технологічний рівень або технологічна інфраструктура кіберзахисту, яка складається з сукупності сил та засобів кіберзахисту. На цьому рівні забезпечується відповідна взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо. Технологічна інфраструктура має три горизонти – національний, галузевий (регіональний) та об'єктовий.

Третій рівень – це базисна інфраструктура кіберзахисту, що забезпечує основні спроможності кіберзахисту. Базисна інфраструктура складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни)», – зазначив під час презентації Олександр Потій, пояснивши також, які передбачені функції та завдання на кожному з цих рівнів.